HP IP Console Switch Software Guide

November 2004 (Third Edition)
Part Number 293671-003

HP IP Console Switch Software Guide

November 2004 (Third Edition)
Part Number 293671-003

Contents

Chapter 7
Using Directory Services Integration (LDAP)

Chapter 8
Accessing Remote Servers

Chapter 9
Managing Remote Servers

About This Guide

This guide provides step-by-step instructions for installation and reference information for operation, troubleshooting, and upgrades for the HP IP Console Switch Viewer.

Audience Assumptions

This document is for the person who installs racks and rack products. This procedure is performed only by trained personnel. HP assumes you are qualified in performing installations and trained in recognizing hazards in rack products.

⚠ Important Safety Information

Before installing this product, read the *Important Safety Information* document included with the product.

Rack Stability

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- **The leveling jacks are extended to the floor.**
- **The full weight of the rack rests on the leveling jacks.**
- **The stabilizing feet are attached to the rack if it is a single-rack installation.**
- **The racks are coupled together in multiple-rack installations.**
- **Only one component is extended at a time. A rack might become unstable if more than one component is extended for any reason.**

Symbols in Text

These symbols might be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents essential information to explain a concept or complete a task.

NOTE: Text set off in this manner presents additional information to emphasize or supplement important points of the main text.

Getting Help

If you have a problem and have exhausted the information in this guide, you can get further information and other help in the following locations.

HP Contact Information

For the name of the nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- In other locations, refer to the HP website at http://www.hp.com.

For HP technical support:

- In North America:
  - — Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - — If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website at http://www.hp.com.
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, refer to the HP website at http://www.hp.com.
- For product-specific information, refer to the following website, http://h18004.www1.hp.com/products/servers/proliantstorage/rack-options/kvm/index-console.html.

Reader's Comments

HP welcomes your comments on this guide. Send your comments and suggestions by e-mail to `ServerDocumentation@hp.com`.

1

Introduction

The HP IP Console Viewer is a cross-platform management application that enables you to view, control, and group console switches and the servers that are attached to them.

The HP IP Console Viewer:

- Ensures compatibility with most popular operating systems and hardware platforms
- Provides secure switch-based authentication, data transfers, and user name and password storage
- Provides directory-based authentication with Microsoft® Active Directory, Light-weight Directory Access Protocol (LDAP), as an available option
- Places system control at the point of need

The HP IP Console Viewer utilizes a Microsoft Windows® Explorer-like navigation with an intuitive split-screen interface, providing you with a single point of access for all your servers. From the HP IP Console Viewer, you can easily perform tasks, such as managing a console switch, launching a video session to a server, or installing new console switches. Built-in groupings, such as Servers, Sites, and Folders, provide an easy way to view select console switches and servers. You can also create custom groupings of console switches and servers by adding folders that store shortcuts. Additional groupings are provided based on the custom fields that you assign.

The HP IP Console Viewer enables you to install, discover, configure, and operate the following products:

- HP 1 x 1 x 16 IP Console Switch
- HP 3 x 1 x 16 IP Console Switch
- HP 1 X 8 KVM Server Console Switch (when tiered and integrated with an HP IP Console Switch using a CAT5 cable)
- HP 2 X 16 KVM Server Console Switch (when tiered and integrated with an HP IP Console Switch using a CAT5 cable)
- Expansion Module
- Interface Adapter (PS/2, universal serial bus (USB), and serial)
- Compaq legacy analog switches (when attached to an Interface Adapter)
  - 1 x 4 [PN: 400336 (-001)(-291)(-B31)]
  - 1 x 8 [PN: 400337 (-001)(-291)(-B31)]
  - 2 x 8 [PN: 400338 (-001)(-291)(-B31)]
  - 2 x 8 (48 VDC) [PN: 400542-B21]

Features and Benefits

- Ease of installation

  Auto discovery of managed console switches enables you to locate and install new console switches. An installation wizard simplifies the task of initial configuration, and an online help application is available to assist you with installation tasks.

- Ease of configuration

  The HP IP Console Viewer has an intuitive GUI-based configuration with tools to load and save managed console switch-based configuration tables and managed console switch groupings.

- Ease of update

  The HP IP Console Viewer contains easy-to-use tools to initiate flash upgrades, distribute database files, and back up and restore managed console switch-based configurations.

- Ease of management

  The HP IP Console Viewer enables you to add and manage multiple console switches and servers in one system. After a console switch or server is installed, you can configure the console switch parameters, control and preempt user video sessions, and execute numerous control functions. From the intuitive Manage Console Switch icon, you can enable Simple Network Management Protocol (SNMP) traps, configure target devices, cascade console switches, and manage user databases.

- Increased customization capabilities

  The HP IP Console Viewer can be customized to meet your specific needs. Unit names, field names, icons, and macros can be customized for maximum flexibility and convenience.

- Increased capacity

  Each managed console switch supports up to 64 internal user accounts and has client support for multiple simultaneous user sessions, depending on the model:

  — 1 x 1, where one user session is supported

  — 3 x 1, where three user sessions are supported

- Increased security

  The HP IP Console Viewer provides secure managed switch-based authentication, data transfers, and user name and password storage. With two levels of access control, Admin and User, you can set target (server) device-specific access rights and interoperate with existing firewalls, virtual private networking (VPN), and NAT-based networks.

Directory Services Integration (LDAP)

The optional Directory Services Integration (LDAP) offers the following features and benefits:

- Authenticates and authorizes users from a shared database
- Controls user privileges (A user can be disabled globally with one change.)
- Enables users to use the same password as they use for the domain
- Does not require manual password synchronization when the user password is changed in the directory; it is changed everywhere
- Manages access controls from a single administration point

Supported Operating Systems

- Microsoft Windows 2000 Workstation
- Microsoft Windows Server 2000
- Microsoft Windows XP (Professional)
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux 2.1 (x86)
- Red Hat Enterprise Linux 3.0 (x86)
- SUSE Linux 8.X and 9.1
- SUSE Enterprise Linux SLES 7, SLES 8, and SLES 9
- Red Hat 8 and 9

Browser Requirements

- Microsoft Internet Explorer 5.5 or higher (Windows operating systems only)
- Mozilla 1.4 or higher

Support Directory Services

Microsoft Active Directory on:

- Windows Server 2000
- Windows Server 2003

System Requirements

The following is a list of the hardware and browser requirements for running the HP IP Console Viewer on the supported operating systems. Configurations with less than the recommended requirements are not supported.

- 500-MHz Intel® Pentium® III
- 256 MB RAM
- 10 or 100 BaseT NIC (100 recommended)
- XGA Video with graphics accelerator (minimum)
- 800 x 600 desktop size (minimum)
- 65,536 (16-bit) colors (recommended)

2

Installation

Before installing the HP IP Console Viewer, refer to the following sections to be sure that you have all the items necessary for proper installation and that you synchronize your mouse pointers.

Setting Up the HP IP Console Switch

1. Adjust the mouse acceleration on each server to none.
2. Install the HP IP Console Switch hardware, connect the Interface Adapters, and connect the keyboard, monitor, and mouse to the analog ports.
3. Connect a terminal or a workstation running emulation software, such as HyperTerminal, to the configuration serial port on the rear panel of the IP Console Switch, and set up the network parameters. You can also set the network parameters from the HP IP Console Viewer.
4. Using the local analog workstation, input all server names through the on-screen display (OSD).

Synchronizing Your Mouse Pointers

Before beginning, synchronize your mouse pointers through the local port, on servers attached to console switches.

NOTE: HP recommends that all Windows systems attached to the console switch use the default Windows PS/2 mouse driver.

Windows Operating Systems

To synchronize the mouse pointers for Windows operating systems (using the default drivers):

1. From the desktop, select **Start>Settings>Control Panel,** and double-click the **Mouse** icon.
2. Select the **Motion** tab.
3. For Windows 2000, set the Speed setting to **50%** (default) and the Acceleration setting to **None.**

   -or-

   For Windows Server 2003, set the set the Speed setting to **50%** (default) and deselect the Enhance Pointer Precision checkbox.

Linux Operating Systems

NOTE: The following Linux example uses Red Hat 3.0. For more information, refer to your Linux operating systems HELP, or documentation.

To synchronize the mouse pointers for Linux operating systems (GNOME):

1. Click **main** menu.
2. From the main menu task list, select **Programs>Settings>Peripherals.**
3. From the Peripherals task list, select **Mouse.** The Mouse Configuration window appears. In this window, you can set the mouse to be either right-handed or left-handed and adjust the mouse motion by changing the threshold and adjusting the acceleration to the fourth position from the far left.

To synchronize the mouse pointers for Linux operating systems (KDE):

1. Go to the main menu, and select **K Menu>KDE Control Center>Input Devices>Mouse.**
2. Set the acceleration to **1X.**
3. Apply the settings, and then click **OK.**

Establishing LAN Connections

To connect an HP IP Console Switch to a network:

NOTE: Although 10Base-T Ethernet can be used, HP recommends a dedicated, switched 100Base-T network for improved performance.

Connect the network cable from the LAN port on the rear panel of the HP IP Console Switch to the network, then power on all attached systems. The following ports must be open on your network for the HP IP Console Viewer to work properly:

- 2068
- 8192
- 3211
- 161

Windows XP SP2 or Newer

To add a console switch without a pre-configured IP address and the client software application is not listed in the Windows XP Firewall Exceptions List, the program must be added to the list of Windows XP Firewall Exceptions, and its scope must be set to the whole Internet.

NOTE: This is the default setting if you choose to unblock when asked at the program startup.

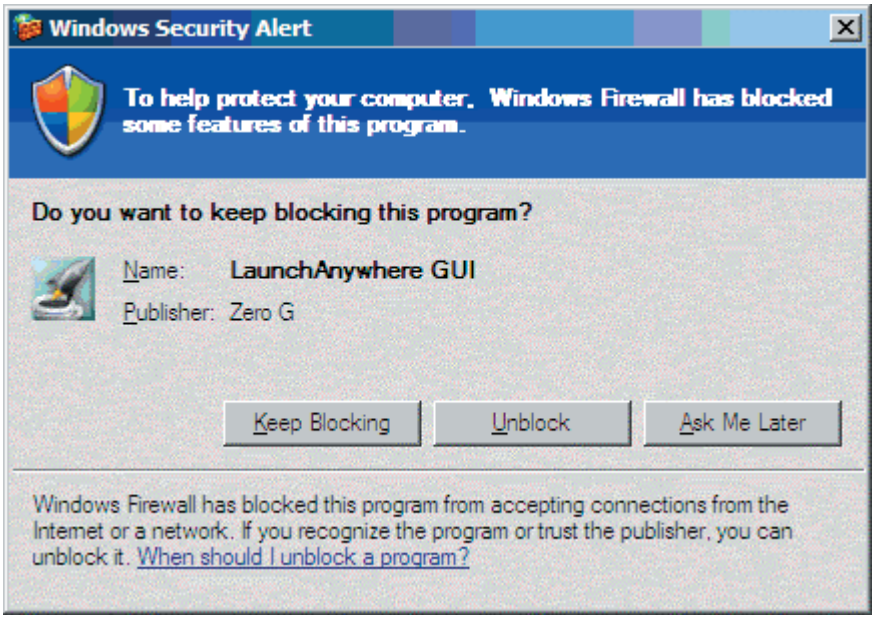

Figure 2-1: Windows Security Alert

Installing the HP IP Console Viewer

To install the HP IP Console Viewer on Windows operating systems:

1. Insert the HP IP Console Viewer CD in to the CD-ROM drive. If AutoMount is supported and enabled, the setup program starts automatically.

   -or-

   If your system does not support AutoMount, set the default drive to the CD-ROM drive letter and execute the following command to start the install program:

   `<CD-ROM drive>:\WIN32\SETUP.EXE`

2. Follow the on-screen instructions.

To install the HP IP Console Viewer on Linux operating systems:

NOTE: The following Linux example uses Red Hat 3.0. For more information, refer to your Linux operating systems HELP, or documentation.

1. Insert the HP IP Console Switch Software CD into your CD-ROM drive. If AutoMount is supported and enabled, proceed to step 2.

   -or-

   If your system does not support AutoMount:

   a. Mount the CD-ROM volume by executing the following command:

      ```
      mount -t iso9660 -ro mode=0555 <device> <mount point>
      ```

      Replace the device with the name of the CD-ROM on your machine and mount point with the name of the desired mount point. For example, to mount a CD-ROM that is the second integrated device electronics (IDE) unit on `/mnt`, execute the command:

      ```
      mount -t iso9660 -ro mode=0555 /dev/hdb /mnt
      ```

   b. At the command prompt, execute the following command to change the working directory to the mount point:

      ```
      cd /mnt
      ```

c. Execute the following command to start the install program:

```
sh ./linux/setup.bin
```

2. Follow the on-screen instructions.

Launching the HP IP Console Viewer

To launch the HP IP Console Viewer on all Windows operating systems, select **Start>Programs>HP IP Console Viewer.**

-or-

From the desktop, double-click the **IP Console Viewer** icon. The HP IP Console Viewer launches.

To launch the HP IP Console Viewer on Linux operating systems:

NOTE: The following Linux example uses Red Hat 3.0. For more information, refer to your Linux operating systems HELP, or documentation.

If the product was installed in the default install directory (/usr/lib/IPViewer), then execute the following command from a shell:

```
./IPViewer
```

-or-

If the product was installed in a directory other than the default, then execute the following command from a shell:

```
<path>/IPViewer
```

-or-

From the desktop, double-click the **HP IP Console Viewer** icon. The HP IP Console Viewer launches.

Configuring the HP IP Console Viewer

IMPORTANT: Before you install the HP IP Console Viewer, go to the following URL to ensure that you have the latest software: http://h18004.www1.hp.com/products/servers/proliantstorage/rack-options/kvm/soft-firmware.html.

1. Install the HP IP Console Viewer on each HP IP Console Viewer client.
2. From one of the HP IP Console Viewer clients, launch the HP IP Console Viewer.
3. Click **New Console Switches** to add the new console switch to the HP IP Console Viewer database. The New Console Switch wizard appears.

   If you previously configured the IP address, select **Yes, the product already has an IP address.**

   -or-

   If you did not configure the IP address, select **No, the product does not have an IP address.** You are prompted to assign an IP address, network mask, and gateway. The HP IP Console Viewer finds the console switch and all Interface Adapters attached to it. These names display in the HP IP Console Viewer main window.
4. Set properties and group servers as desired into Sites or Folders through the main window.
5. Create user accounts by clicking the **Manage Console Switch** icon.
6. After one HP IP Console Viewer client is configured, select **File>Database>Save** to save a copy of the database with all the settings.
7. From the second HP IP Console Viewer client, click **File>Database>Load,** and browse to find the file you saved.
8. If the local analog workstation (through the OSD) adds, deletes, or renames any Interface Adapters after you loaded this file, resynchronize your local database with the OSD by clicking **Manage Console Switch** icon and clicking **Resync** under **Settings>Servers.**
9. To access a server attached to your HP IP Console Switch, select the desired server in the main window, and click **Launch KVM Session** to launch a server session.

10. Adjust the resolution by selecting **View>Auto Scale,** and click the **Maximize** button. Select **Tools>Automatic Video Adjust** of the server video in the **Video Session Viewer.**
11. After setting the mouse properties, click the **mouse synchronization** button in the HP IP Console Viewer menu bar.

3

Navigating the HP IP Console Viewer

The HP IP Console Viewer consists of several components: the main window, the Manage Console Switch window, and the Video Session Viewer component. After you launch the HP IP Console Viewer, the main window displays. The main window enables you to view, access, manage, and create custom groupings for all the supported units in the data center.

When you select a target device, you can click the **Launch KVM Session** button in the main window to launch the Video Session Viewer. This component enables you to control the keyboard, monitor, and mouse functions of individual servers.

When you select a console switch, you can click the **Manage Console Switch** button in the main window to launch the Manage Console Switch window. This window enables you to configure and control the console switch.

Viewing the Main Window

The main window is divided into several different views. These views change based on the type of devices selected or the task you want to complete. Click one of the views to see your system organized by categories, such as console switches, servers, sites, or folders. The default display for the main window can be configured by the user. By default, each time you launch the main window, it reads the local database to determine which view to display.

Main Window Features

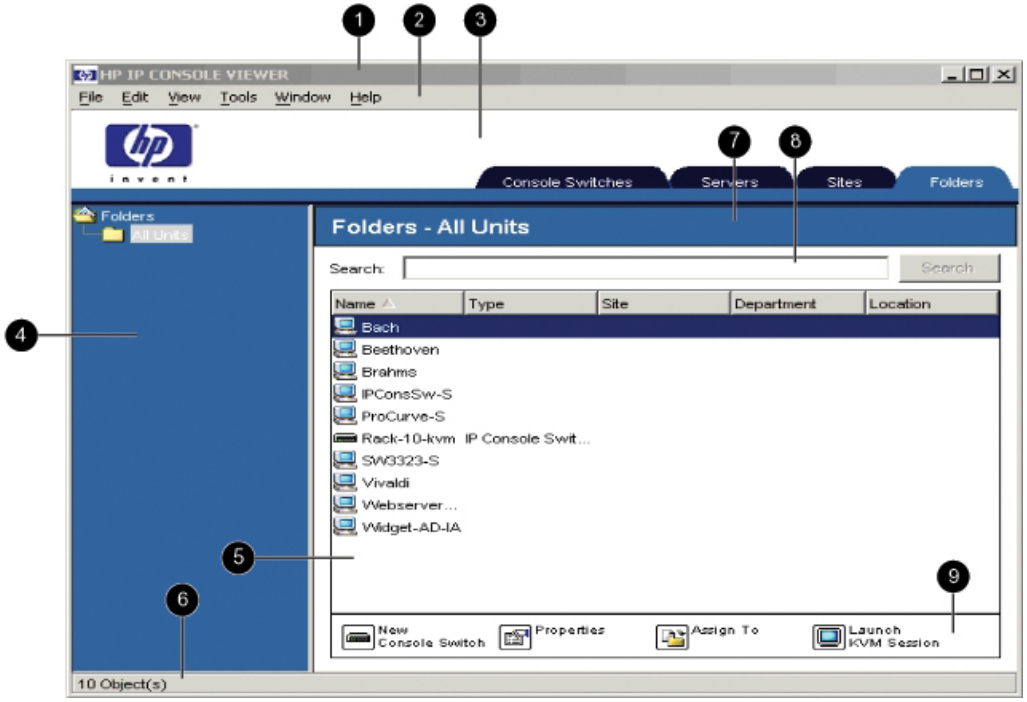

Figure 3-1: Main window features

Position	Feature	Function
1	Title bar	Provides the title of the software.
2	Menu bar	Contains six menus (File, Edit, View, Tools, Window, and Help).

continued

Figure 3-1: Main window features *continued*

Position	Feature	Function
3	View Selector Tabs	Contains four tabs (Console Switches, Servers, Sites, and Folders).
4	Group view	Contains a tree view representing the groups that are selected from the icon view. The group view also controls what appears in the selected view.
5	List view	Displays a list in the currently selected group view or the results of a search executed from the search bar.
6	Status bar	Displays the number of items shown in the list view.
7	Selected view	Displays the search bar, list view, and task window.
8	Search bar	Enables you to filter the list view displayed in the selected view, based on the text entered.
9	Task window	Contains buttons representing tasks that can be executed. Some buttons are dynamic, based on the type of items selected in the list view, and other buttons are fixed and always present.

4

Adding and Discovering Console Switches

Adding Console Switches

Before a console switch can be accessed through the HP IP Console Viewer, you must add it to the HP IP Console Viewer database. After the console switch has been manually added or discovered, it appears in the list view.

If an IP address has already been assigned to the console switch, the HP IP Console Viewer automatically discovers it by searching for an exact IP address or an address range. If an IP address has not been assigned, you must manually add the console switch. If you are installing multiple console switches, then HP recommends using the Discover Wizard. If you are installing a single console switch, then HP recommends using the New Console Switch Wizard.

NOTE: HP recommends that you assign names to the target servers in the HP IP Console Switch OSD interface before adding them to the HP IP Console Viewer.

Adding a Console Switch without an Assigned IP Address

1. Select **File>New>Console Switch,** or click the **New Console Switch** icon. The New Console Switch Wizard appears.

Figure 4-1: New Console Switch Wizard

2. Click **Next.** The Product Type window appears.

Figure 4-2: Product Type window

3. Select a product from the product list. The IP Address window appears.

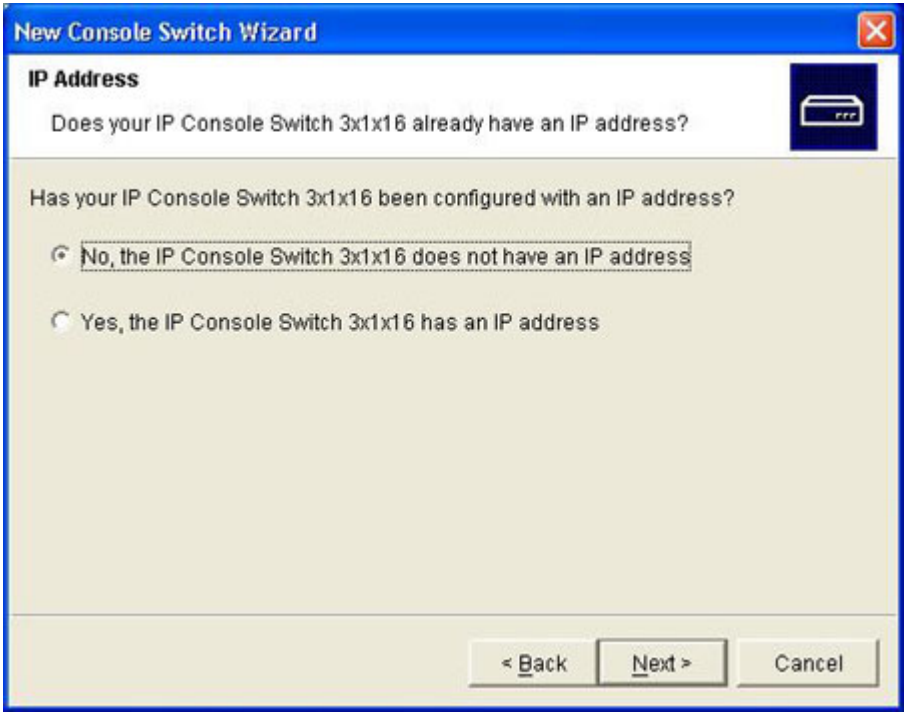

Figure 4-3: IP Address window

4. Indicate that the HP IP Console Switch does not have an IP address assigned by selecting **No,** and click **Next.** The Network Address window appears.

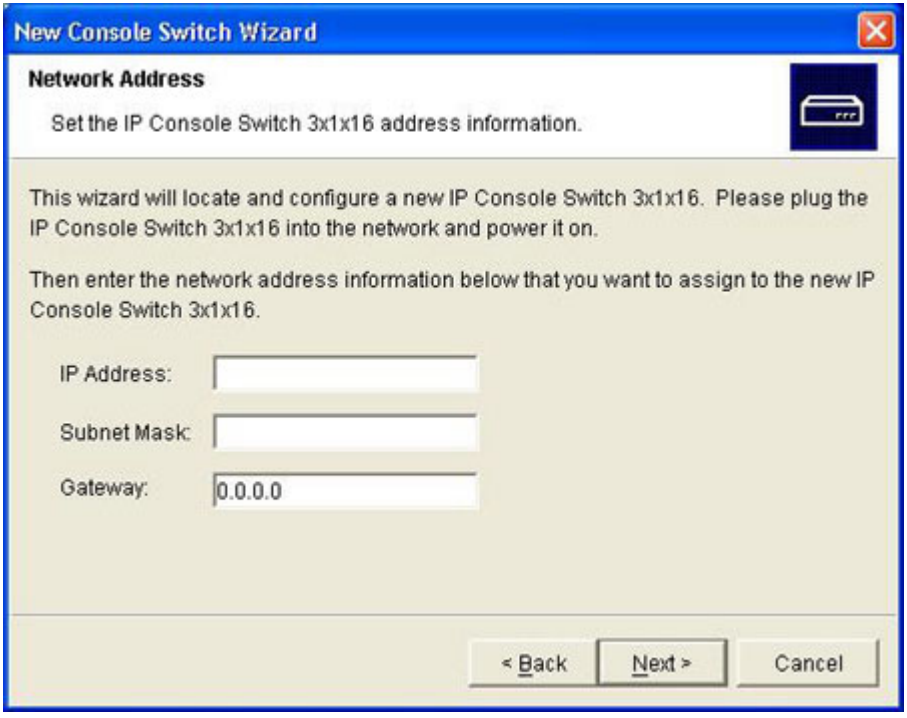

Figure 4-4: Network Address window

5. Enter the IP address, subnet mask, and gateway for the HP IP Console Switch, and click **Next.** The HP IP Console Viewer searches for the console switch and all Interface Adapter IDs and server names associated with the particular console switch. The Found window appears.

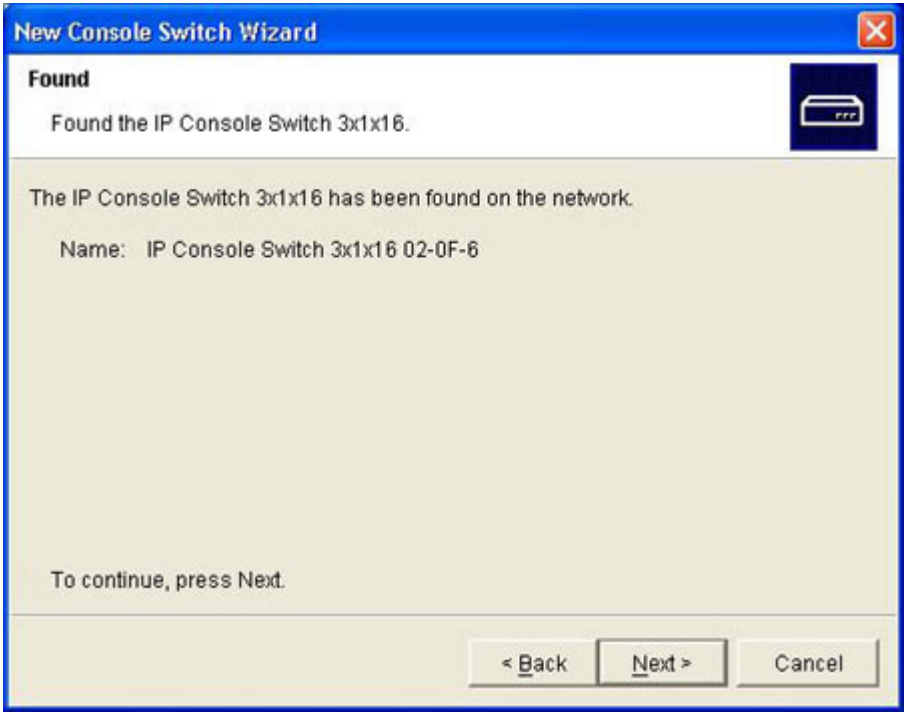

Figure 4-5: Found window

6. Click **Next.** If a cascade legacy analog console switch attached to an Interface Adapter is detected, then the Enter Cascade Switch Information window appears.

   a. The Assign Cascade Switch dialog box displays a list of all the Interface Adapters attached to a cascade switch. Associate the appropriate console switch from the dropdown list for each Interface Adapter that has a console switch attached.

   b. The Existing Cascade Switches dialog box contains a list of all the current console switches defined in the database. Click **Add, Modify,** or **Delete** to alter the list.

      The HP IP Console Viewer only searches for the amount of servers designated by the console switch type (user definable).

      After a cascade switch has been added to an Existing Cascade Switches list, you can modify or delete the cascade switch displayed by selecting the cascade switch and clicking **Modify** or **Delete.**

-or-

If no cascade switches attached to any Interface Adapters were detected, then the Completing Wizard window appears. Click **Finish** to exit and return to the main window.

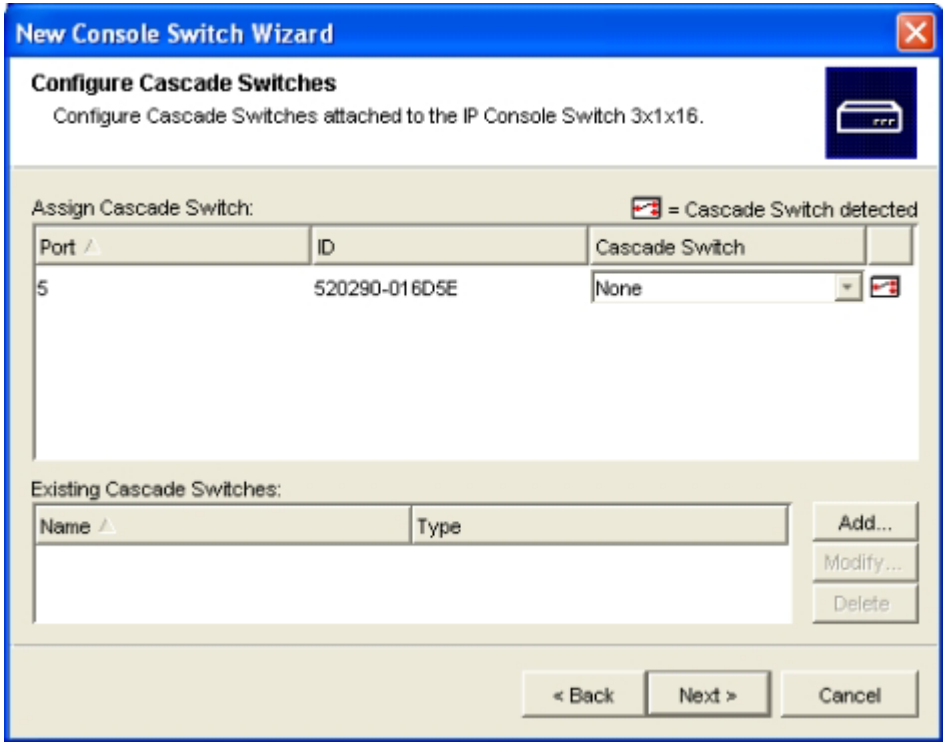

Figure 4-6: Enter Cascade Switch Information window

7. Click **Next.** The Completing the New Console Switch Wizard window appears.
8. Click **Finish** to exit and return to the main window. The console switch displays in the list view.

Adding a Console Switch with an Assigned IP Address

1. Select **File>New>Console Switch,** or click the **New Console Switch** icon. The New Console Switch Wizard window appears.
2. Click **Next.** The Product Type window appears.
3. Select a product from the product list, and click **Next.** The IP Address window appears.

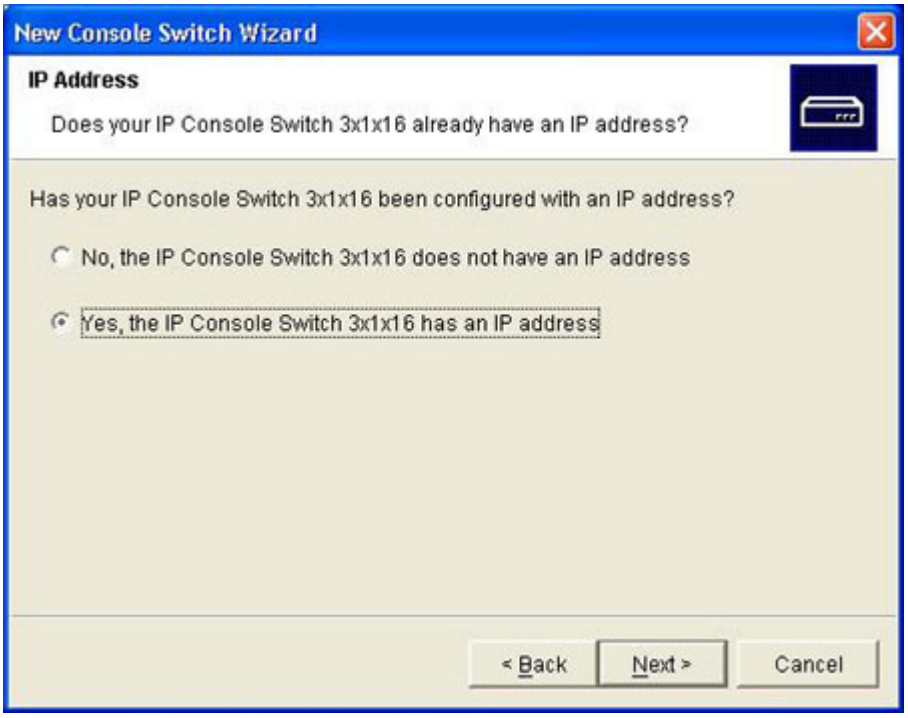

Figure 4-7: IP Address window

4. Indicate that the HP IP Console Switch has an IP address assigned to it by selecting **Yes,** and click **Next.** The Locate IP Console Switch window appears.

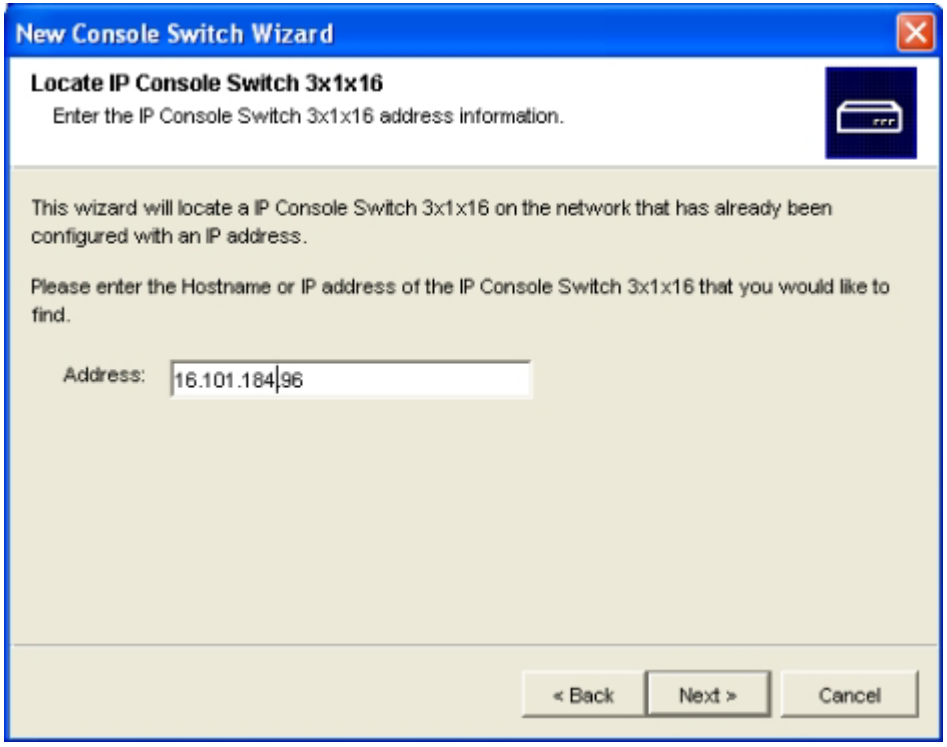

Figure 4-8: Locate IP Console Switch window

5. Enter the HP IP Console Switch IP address or DNS name, and click **Next.** The IP Console Viewer searches for the console switch and all Interface Adapter IDs and server names associated with the particular console switch. The Found window appears.

6. Click **Next.** If a cascade legacy analog console switch attached to at least one Interface Adapter is detected, then the Enter Cascade Switch Information window appears.

   a. The Assign Cascade Switch dialog box displays a list of all the Interface Adapters attached to a cascade switch. Associate the appropriate console switch from the dropdown list for each Interface Adapter that has a console switch attached.

   b. The Existing Cascade Switches dialog box contains a list of all the current console switches defined in the database. Click **Add, Modify,** or **Delete** to alter the list.

      The IP Console Viewer only searches for the amount of servers designated by the console switch type (user definable).

      After a cascade switch has been added to an Existing Cascade Switches list, you can modify or delete the cascade switch displayed by selecting the cascade switch and clicking **Modify** or **Delete.**

      -or-

      If no cascade switches attached to any Interface Adapters were detected, then the Completing Wizard window appears. Click **Finish** to exit and return to the main window.

7. Click **Next.** The Completing the New Console Switch Wizard window appears.

8. Click **Finish** to exit and return to the main window. The console switch displays in the list view.

Discovering a Console Switch

1. Select **Tools>Discover.** The Discover Wizard window appears.

Figure 4-9: Discover Wizard window

2. Click **Next.** The Enter Address Range window appears.

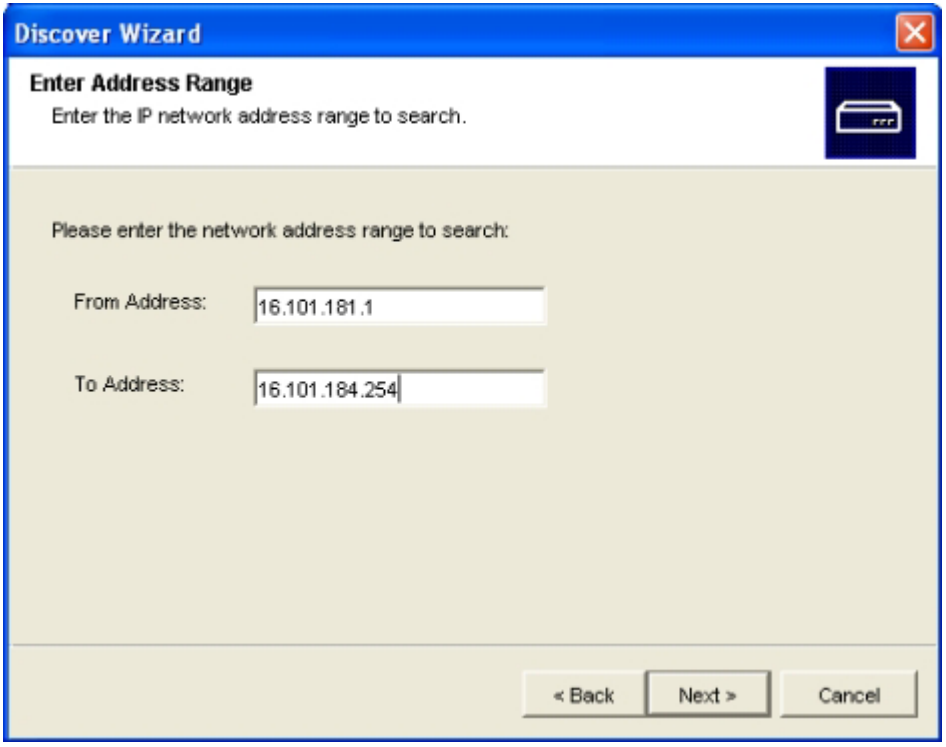

Figure 4-10: Enter Address Range window

3. Enter a valid range of network IP addresses to search on the network in the From Address: and To Address: fields. Use the IP address dot notation `xxx.xxx.xxx.xxx`.
4. Click **Next.** The Searching Network window appears. Progress text indicates how many addresses have been probed from the total number specified by the range and the number of IP Console Switches found.

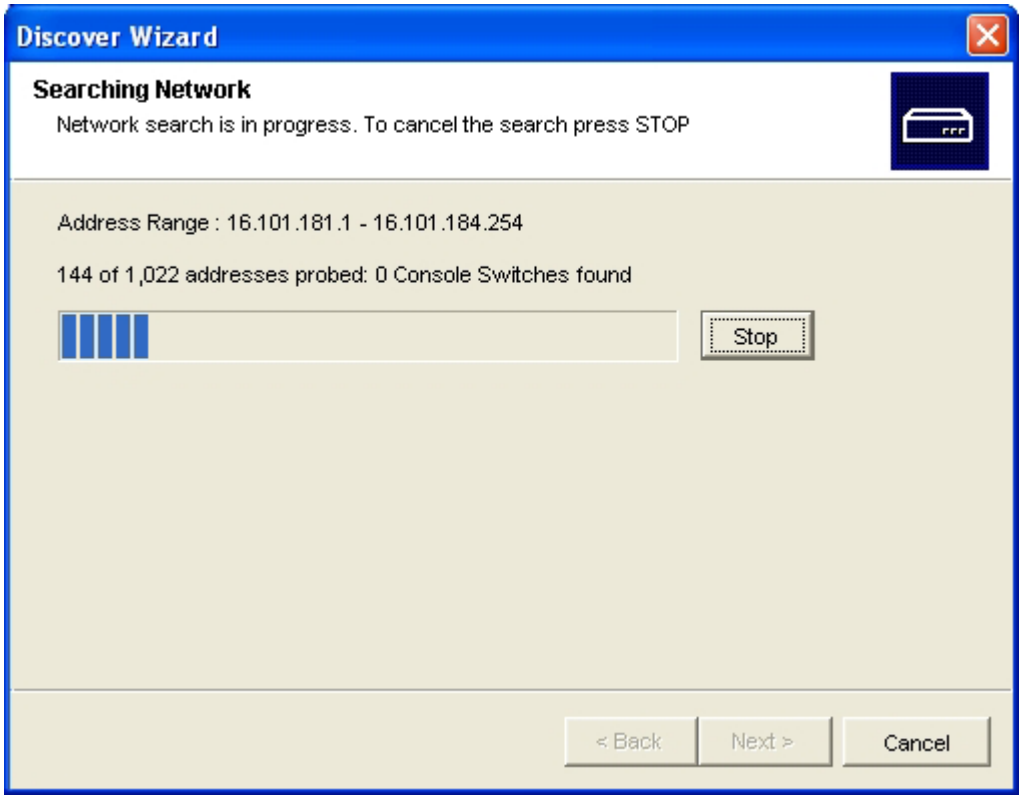

Figure 4-11: Searching Network window

5. If one or more new console switches are discovered, the Select Console Switches window appears. From this window, you can select the console switches to add to the local database. Continue to step 6.

   -or-

   If no new console switches are found or if you pressed **Stop** during the add process, the Discover Wizard was unsuccessful window appears. Click **Finish** to exit. You must add the console switch manually. For more information, refer to the section, "Adding a Console Switch without an Assigned IP Address" in this chapter.

Figure 4-12: Select Console Switches window

6. Select the console switches to add from the Console Switch Found: box, and click the **>** button to move the selection to the Console Switches to add: box. Repeat for all console switches you want to add.
7. Click **Next.** The Adding Console Switches window appears. A progress bar appears while new console switches are added to the list.

   When all the selected console switches have been added to the local database, the Completing the Discover Wizard window appears. Click **Finish** to exit and return to the main window. The new console switches are displayed in the list view.

   The Discover Wizard does not automatically find servers attached to the console switch. After running the Discover Wizard, click **Resync** in the Manage Console Switch to find servers attached to the console switch.

   -or-

   If one or more console switches could not be added to the local database for any reason, including if you pressed **Stop** during the add process, the Discover Wizard Not All Console Switches Added page appears. This page lists all of the console switches that you selected and the status for each. The status is indicated if a console switch was added to the local database and if not, why the process failed. Click **Done** when you are finished reviewing the list.

   NOTE: If a console switch already exists in the local database with the same IP address as a discovered console switch, then the discovered console switch is ignored and is not displayed on the next Discover Wizard window.

5

Accessing Console Switches

When you click the Console Switches icon, you see a list of the console switches currently defined in the local database.

To access a console switch, first log in with a valid password and user name. After you have logged in to the console switch, the HP IP Console Viewer caches the user name and password into memory for the duration of the HP IP Console Viewer session. All HP IP Console Switch Viewer communications to the console switch use a secure management protocol (SMP).

NOTE: You can clear the login credentials. For information on clearing login credentials, refer to the "Clearing Login Credentials" section in this chapter.

To access a console switch:

1. Click the **Console Switches** icon to display the console switches in the selected view.
2. Double-click the desired console switch. A login dialog box appears.

   -or-

   Select the console switch, and select the **Manage Console Switch** icon. A login dialog box appears.

   -or-

   Right-click the console switch, and select the **Manage Console Switch** icon from the resulting list. A login dialog box appears.

   -or-

Click the **Console Switches** icon, and press the **Enter** key. A login dialog box appears.

3. Enter a valid user name and password. If a new user name and password have not been created, the Override Admin account can be used. The default user name, for this account, is `Admin` (case-sensitive) and the default password field is blank.

   IMPORTANT: If you previously logged in to the console switch during the same IP Console Viewer session, the login dialog does not appear, since the cached credentials are used.

4. Click **OK.** The Manage Console Switch window appears. For information on managing console switches, refer to Chapter 9.

   -or-

   Click **Cancel** to exit without logging in.

Clearing Login Credentials

The clear login credentials feature clears the cached login credentials, if present, and forces the login prompt to redisplay the next time you launch the Video Session Viewer or Manage Console Switch.

To clear login credentials:

1. Select **Tools>Clear Login Credentials.** A message appears.
2. Click **OK** to exit.

6

Managing Console Switches

After you have installed a new console switch, you can view and configure unit parameters, view and control currently active video sessions, and execute a variety of control functions, such as rebooting and upgrading your console switch. The Manage Console Switch window consists of the Settings, Status, and Tools tabs.

Viewing and Configuring Console Switch Parameters

The Settings tab enables you to display an expandable list of categories covering a wide range of parameters for the HP IP Console Switch. When a category is selected, the parameters associated with that category are read from the console switch, the database, or both. You can then modify those parameters and send changes securely back to the HP IP Console Switch through the Secure Management Protocol.

Changing Global, Network, Session, and Authentication Parameters

The Global category enables you to view the Product Type, Serial Number, and the Language settings for the HP IP Console Switch.

The Serial Number (EID) field contains information for the HP IP Console Switch hardware and the EID attached to that console switch.

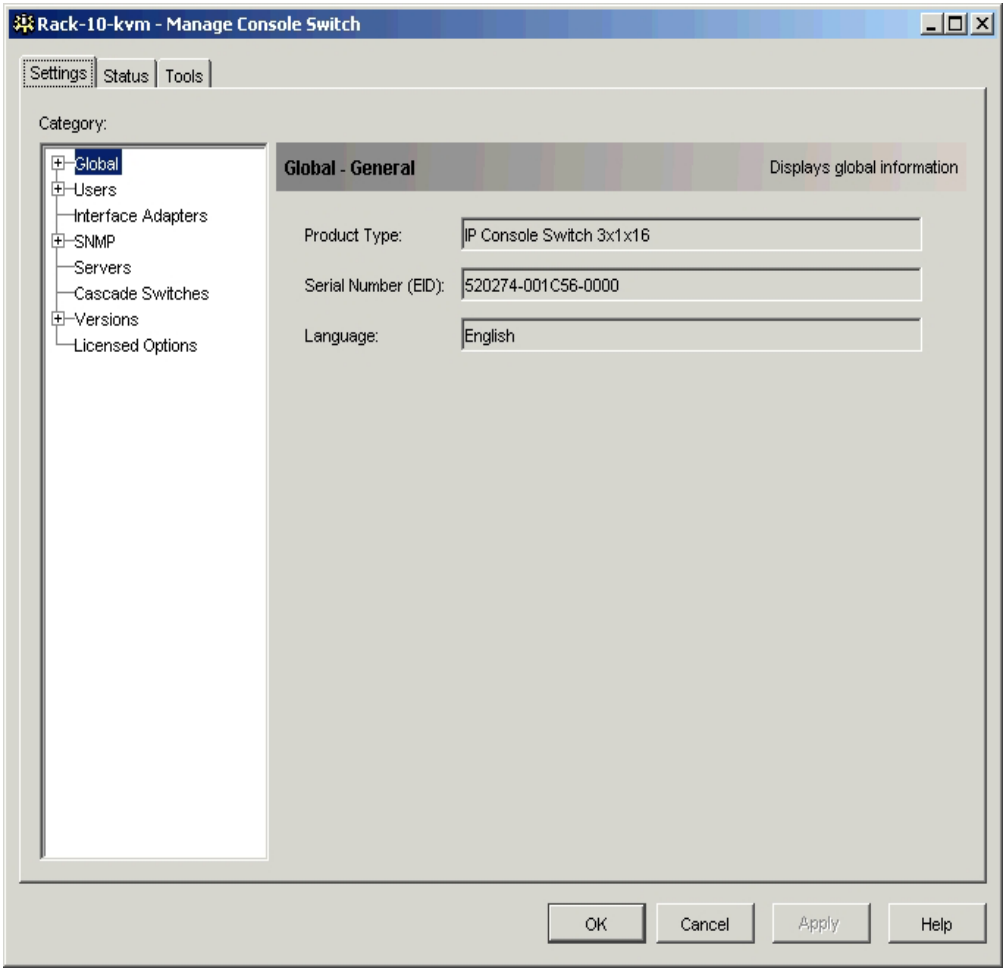

Figure 6-1: Global category

The Network subcategory enables you to view the network settings of a console switch, including the Name (read-only), IP Address, Subnet Mask, Gateway, MAC Address (read-only), LAN Speed, DNS Servers, and Bootp settings.

The DNS servers are used to find domain controllers during LDAP authentication and authorization operations.

The DNS Server fields only appear if LDAP Authentication is licensed on this IP console switch.

NOTE: If the IP address is changed in this subcategory, the IP address under the console switch Properties window must also be changed to have full functionality.

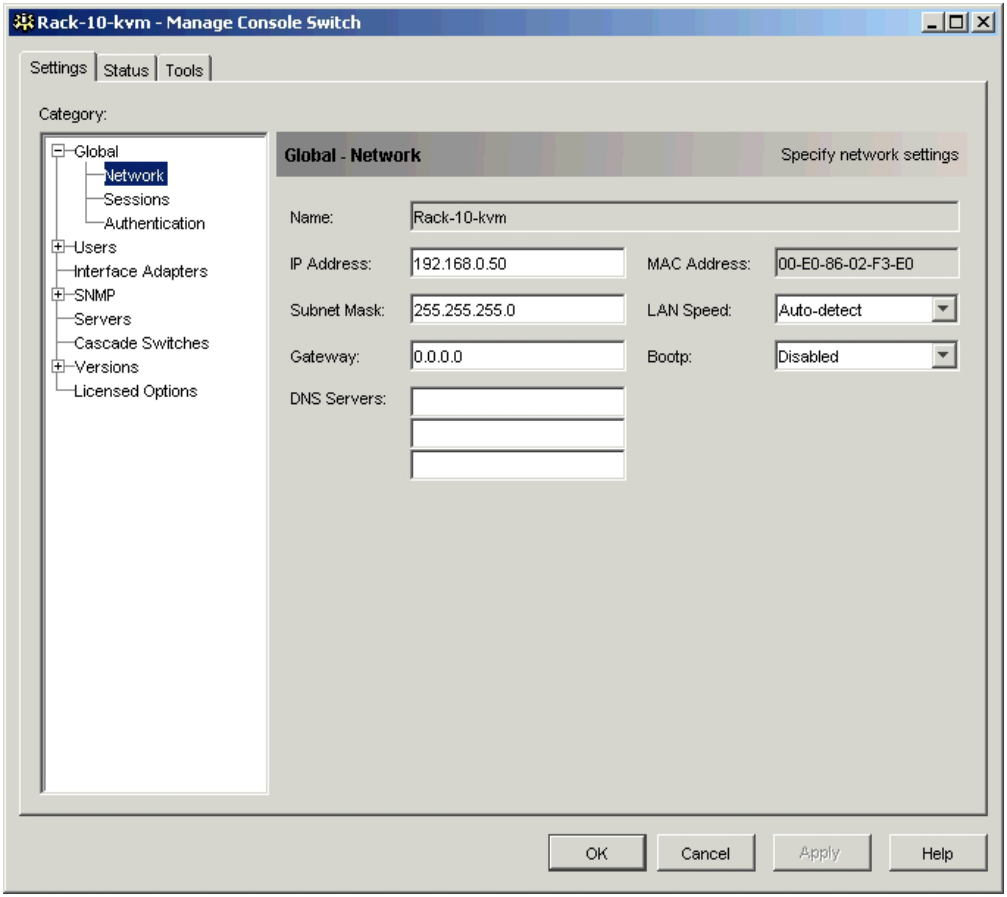

Figure 6-2: Network subcategory

The Sessions subcategory enables you to specify the active Video Session Timeout, which configures the console switch to close an inactive video session after a specified number of minutes.

This subcategory also enables you to configure the preemption warnings settings. Enabling the Video session preemption timeout option enables you to specify the time (5 to 120 seconds) for which a preemption warning message appears before a video session is preempted. If this option is not enabled, preemption occurs without warning.

You can also set the Secure Socket Layer (SSL) encryption levels to use for the encryption of keyboard and mouse data of all video sessions to the console switch.

NOTE: The highest encryption level will be used, based on the following order (highest to lowest):

- 128-bit encryption
- Triple Data Encryption Standard (3DES)
- Data Encryption Standard (DES)

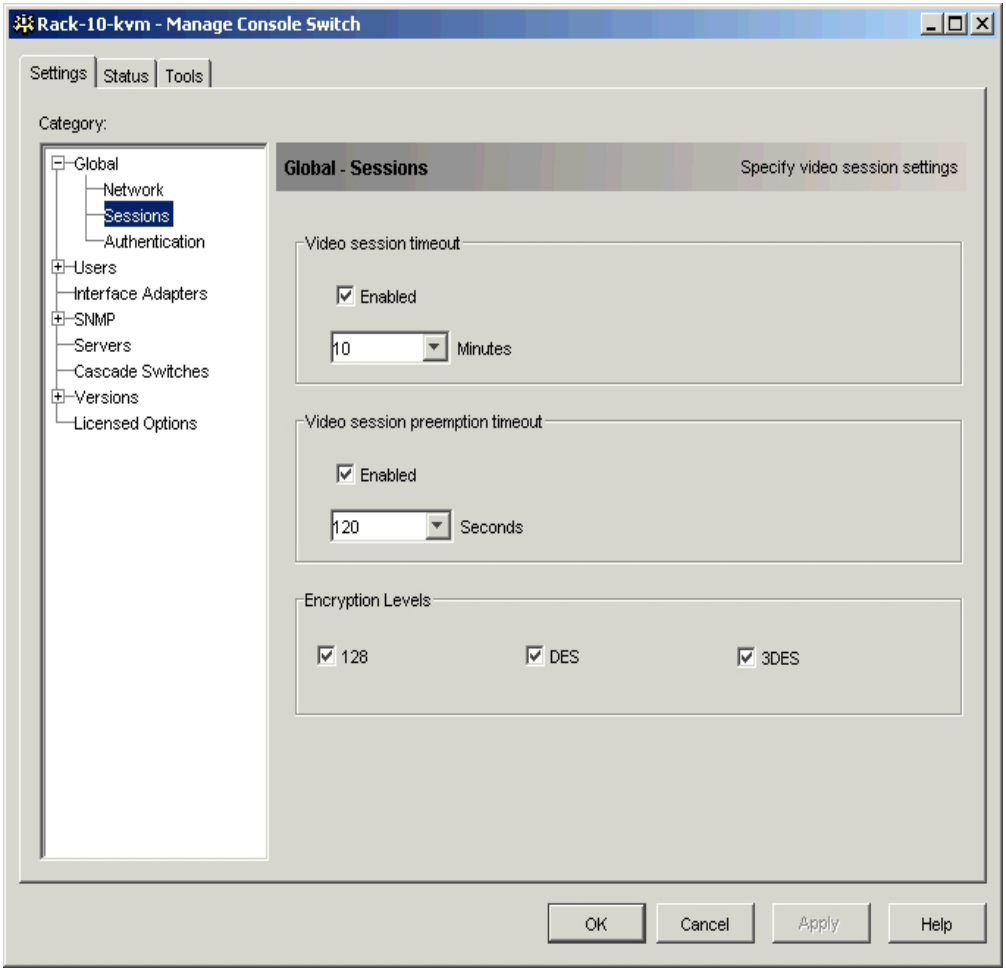

Figure 6-3: Sessions subcategory

Selecting the Authentication Parameters

The Authentication subcategory enables you to select the type of authentication method to be used.

IMPORTANT: Before implementing LDAP functionality, refer to Appendix A for a better understanding of how LDAP works.

NOTE: The LDAP Authentication is not available until a valid license key is installed. For information on purchasing and installing license keys, refer to Chapter 7 of this guide.

The three different types of authentication methods are:

- **Local Authentication** (with local access control)—Provides secure managed switch based authentication, data transfers, and user name and password storage. With two levels of access control, Console Switch Admin and User, you can set target device-specific access rights and interoperate with existing firewalls, VPNs, and NAT-based networks. This is the default setting and has the same functionality as in the previous software releases.

  NOTE: The previous release of console switches came pre-configured with one default Console Switch Admin user. This default user has been replaced in this release by the Override Admin account.

- **LDAP Authentication Only** (with local Access Control List [ACL])—Provides a secure managed server-based authentication for passwords and user names and a local switch-based authentication for ACLs. ACLs are maintained and stored in each individual console switch, while user accounts must be maintained in the console switch and in the directory server. Passwords are only in the directory server. For more information on LDAP, refer to Chapter 7 of this guide.

- **LDAP Authentication and Access Control**—Provides a secure managed server-based authentication for user names and passwords. User rights and user accounts are stored in the Active Directory with directory controls centralized in the ACL. For more information on LDAP Access Control, refer to Chapter 7 of this guide.

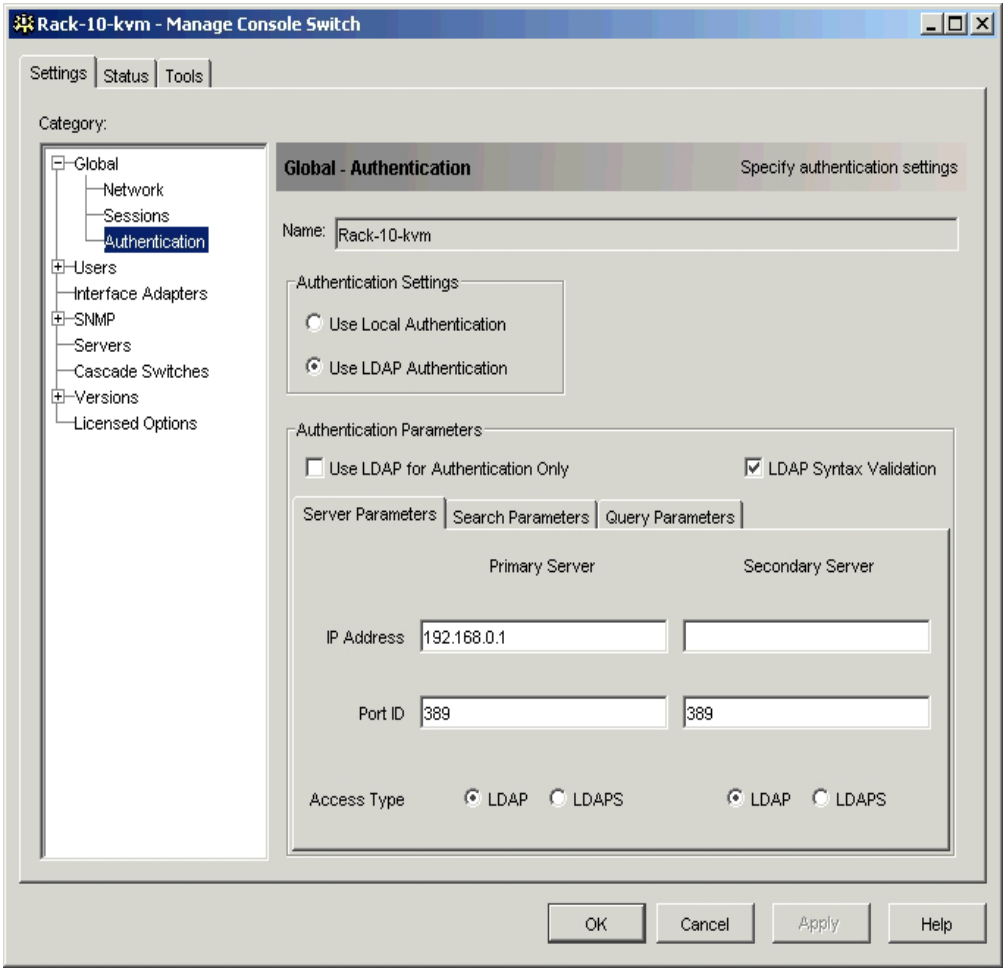

Figure 6-4: Authentication subcategory

Setting User Accounts

The Users category enables you to configure user accounts. There are two types of user accounts, internal or external. Internal accounts, such as Local Authentication accounts, reside within the console switch, while external accounts, such as LDAP Authentication and Access Control accounts, are stored in the active directory.

When you select the Users category for the first time, the Manage Console Switch function retrieves and displays user information and current access levels based on the type of authentication you have selected.

- When Local Authentication or LDAP Authentication Only modes are enabled, the Manage Console Switch retrieves and displays a list of user names and current access levels from the console switch.

  Through the Users category, when Local Authentication or LDAP Authentication Only modes are enabled, you can:

  — Add, modify, or delete users in this listing

  — Assign access levels: Console Switch Admin or User

  — Assign individual server access rights to a user through the User Access Level function

  — Enable the Security Lock-out feature that can lock out users if they try to enter an invalid password five consecutive times (This feature enables you to configure the Security Lock-out settings, as well as unlock any users.)

  NOTE: The Security Lock-out feature only applies to Local authentication. When LDAP authentication is used, the lockout functionality of the directory service must be used.

- When LDAP Authentication and Access Control mode is enabled, the user names and current access levels are stored in, and managed from, the active directory.

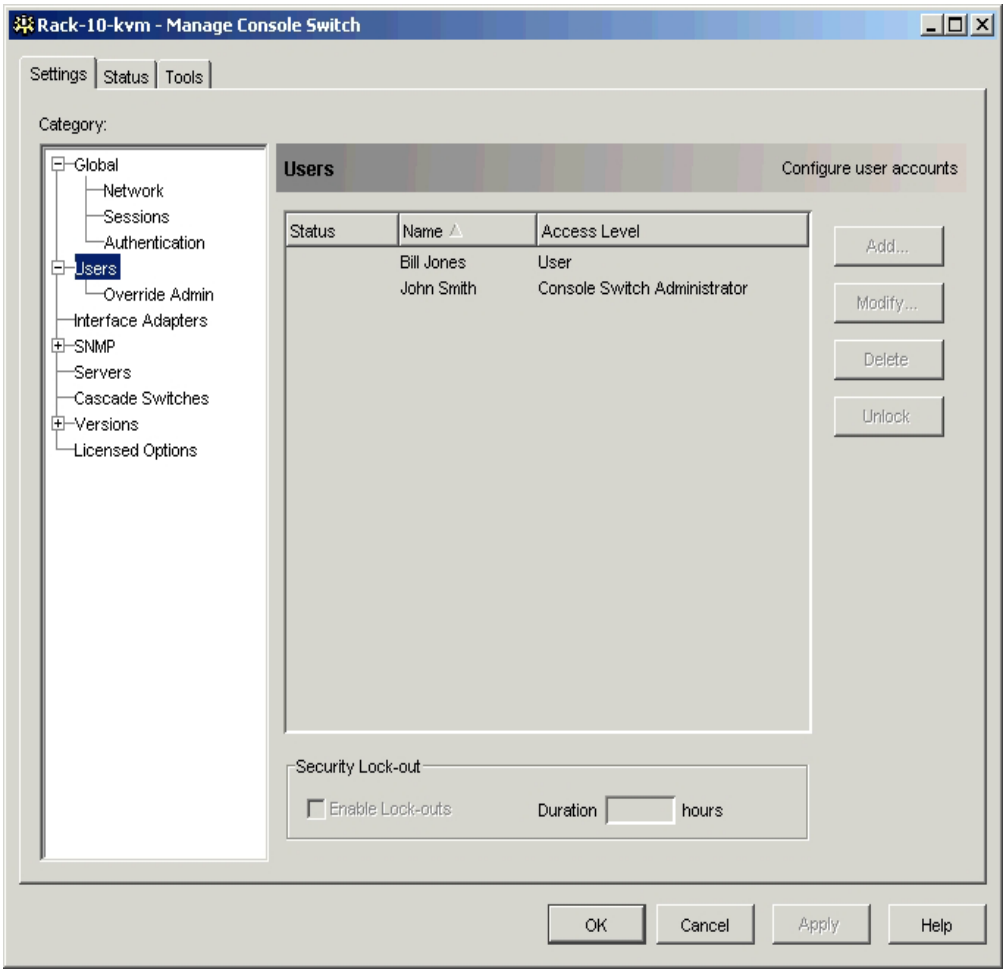

Figure 6-5: Users category

Table 6-1: User Access Level Rights

Operations	Console Switch Admin	User
Preemption	All	No
Configure Global and Network settings (security mode, timeout, and SNMP)	Yes	No
Reboot	Yes	No
Upgrade	Yes	No
Administer user accounts	Yes	No
Configure port settings	Yes	No
Monitor server status	Yes	No
Target device access	Yes	Assigned by admin
Server resync	Yes	Yes

Configuring User Accounts

Adding or Modifying a Local Authentication User

1. Select the user in the Users category.
2. Click **Add** to add a new user. The Add User dialog box appears.

   -or-

   Click **Modify** to modify a current user. The Modify User dialog box appears.

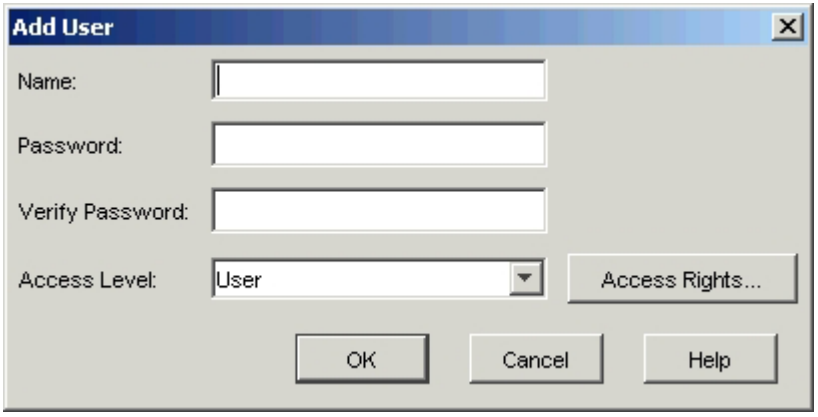

Figure 6-6: Add User dialog box

3. Enter the user name and password (user assigned), and verify the password by entering it again in the Verify Password field.

   IMPORTANT: Passwords must be between 5 and 16 characters in length, contain both alphabetic and numeric characters, and contain both uppercase and lowercase alphabetic characters.

   IMPORTANT: User names must be between 1 and 16 characters. If you intend on using the optional LDAP functionality in the future, be sure to follow the Microsoft Active Directory user account rules when creating a user name.

   NOTE: The Access Rights button is only enabled when Access Level = User is selected.

4. Select the appropriate access level for the user from the Access Level dropdown list. If you select the User option, the Access Rights button activates.
   a. Click **Access Rights** to select individual servers for that user. The User access rights dialog box appears.
   b. From the left column, select one or more servers for which this user should have access rights. Click **Add.**
   c. From the right column, select one or more servers from which to remove a user's access rights. Click **Remove.**
   d. Repeat steps b and c until the right column represents the appropriate server access for this user, and click **OK.**

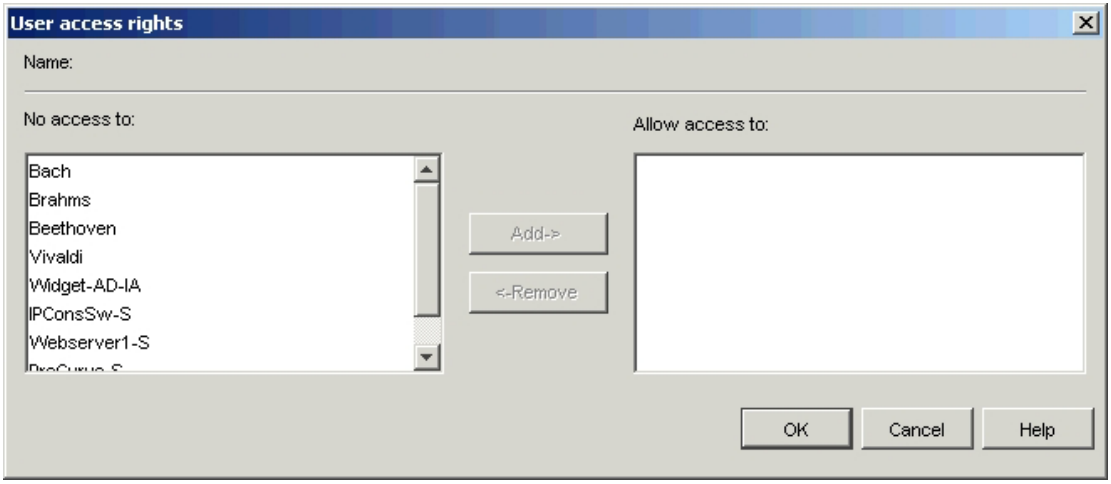

Figure 6-7: User access rights dialog box

5. Click **OK** to save the settings and return to the main window, or click **Cancel** to exit.

Adding or Modifying an LDAP Authentication Only User

NOTE: For LDAP Authentication and Access Control users, add user accounts and passwords in the active directory.

1. Select the user in the Users category.

IMPORTANT: The user name in the Users category must be the same as the display name in the active directory.

2. Click **Add** to add a new user. The Add User dialog box appears.

   -or-

   Click **Modify** to modify a current user. The Modify User dialog box appears.

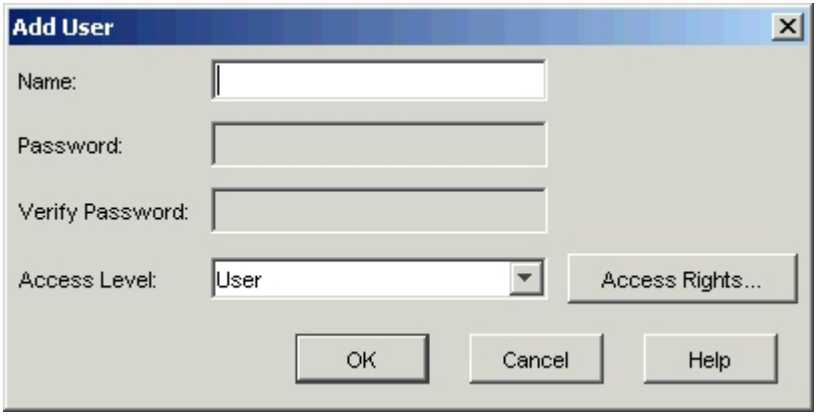

Figure 6-8: Add User dialog box

3. Select the appropriate access level for the user from the Access Level dropdown list. If you select the User option, the Access Rights button activates.
   a. Click **Access Rights** to select individual servers for that user. The User access rights dialog box appears.
   b. From the left column, select one or more servers for which this user should have access rights. Click **Add.**
   c. From the right column, select one or more servers from which to remove a user's access rights. Click **Remove.**
   d. Repeat steps b and c until the right column represents the appropriate server access for this user, and click **OK.**

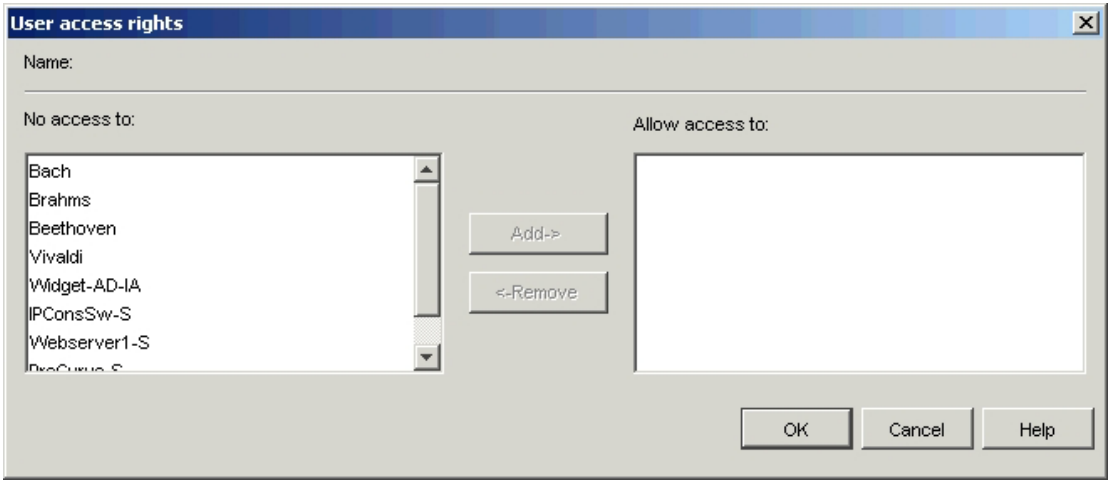

Figure 6-9: User access rights dialog box

4. Click **OK** to save the settings and return to the main window, or click **Cancel** to exit.

Deleting a User

1. Select the user in the Users category.
2. Click **Delete.** The Confirm Deletion dialog box appears.
3. Click **Yes** to confirm the deletion, or click **No** to exit the window without deleting the user.

Locking and Unlocking User Accounts

If the console switch is configured for Local Authentication, and a user enters an invalid password five consecutive times, the Security Lock-out feature temporarily disables that account. If a user attempts to log in again, an error message appears from the software client application. All local accounts, except the Override Admin account are subject to this lock-out policy.

An admin can specify the number of hours (1 to 99) that accounts are locked. When Enable Lock-outs is not selected, the Security Lock-out feature is disabled, and no users can be locked out.

If an account becomes locked, it remains locked until the number of hours specified in the Duration field has elapsed, the console switch is power cycled, or an administrator unlocks the local account using the Unlock function on this panel.

NOTE: If your account is locked and you have LDAP Authentication and Access Control enabled, your account must be unlocked through the active directory. Contact your active directory administrator for further details.

Unlocking an Account

1. Select the **Users** category.
2. Click **Unlock.** The lock icon next to the user name disappears.
3. Click **OK** or **Apply.** The user can to log in again.

   -or-

   Click **Cancel** to exit without saving.

Specifying Security Lock-Out Time

1. Select the **Users** category.
2. Select the **Enable Lock-outs** checkbox.
3. Enter the number of hours that a user is locked out (1 to 99) in the **Durations** field.
4. Click **Apply,** and then click **OK.**

Disabling Security Lock-Out

1. Select the user in the Users category.
2. Deselect **Enable Lock-outs** checkbox.
3. Click **Apply,** and then click **OK.**

NOTE: Disabling Security Lock-out has no effect on users who are already locked out.

Override Admin

Override Admin is the one account that can be used to get into the console switch from a network, even if the local accounts are locked or don't exist or if LDAP is not working properly. The Override Admin account is a permanent account that cannot be deleted. It has the same access right privileges as a Console Switch Admin. The ID and password should be closely held by authorities and should not be used as Admin or User accounts on a day-to-day basis. The Override Admin account name and password settings are only accessible to the Override Admin user (i.e., must be logged in as the Override Admin to access this panel. To access the Override Admin settings, access the **Users** category and then select **Override Admin.**

NOTE: When upgrading from a pre-3.0.0 firmware version, the upgrade procedure will search for an existing Console Switch Admin account named "Admin" and migrate this username and password to be the default Override Admin account. If the user "Admin" is not found, then the default Override Admin username will be "Admin" and the default password will not be set (empty).

Viewing Interface Adapters

The Interface Adapters category displays a list of Interface Adapters attached to the HP IP Console Switch and their statuses, as well as the Port, Interface Adapter ID, Type, and Language. A green circle indicates that the Interface Adapter is online. A yellow circle indicates that the Interface Adapter is being upgraded, and a red X indicates that the Interface Adapter is offline. To clear offline adapters, click the **Clear Offline** button, and then click **OK** when prompted to confirm.

NOTE: The Interface Adapter Status, Port, ID, Type, and Language columns can be sorted by selecting the column name.

NOTE: The Clear Offline button is only enabled if at least one Interface Adapter is offline.

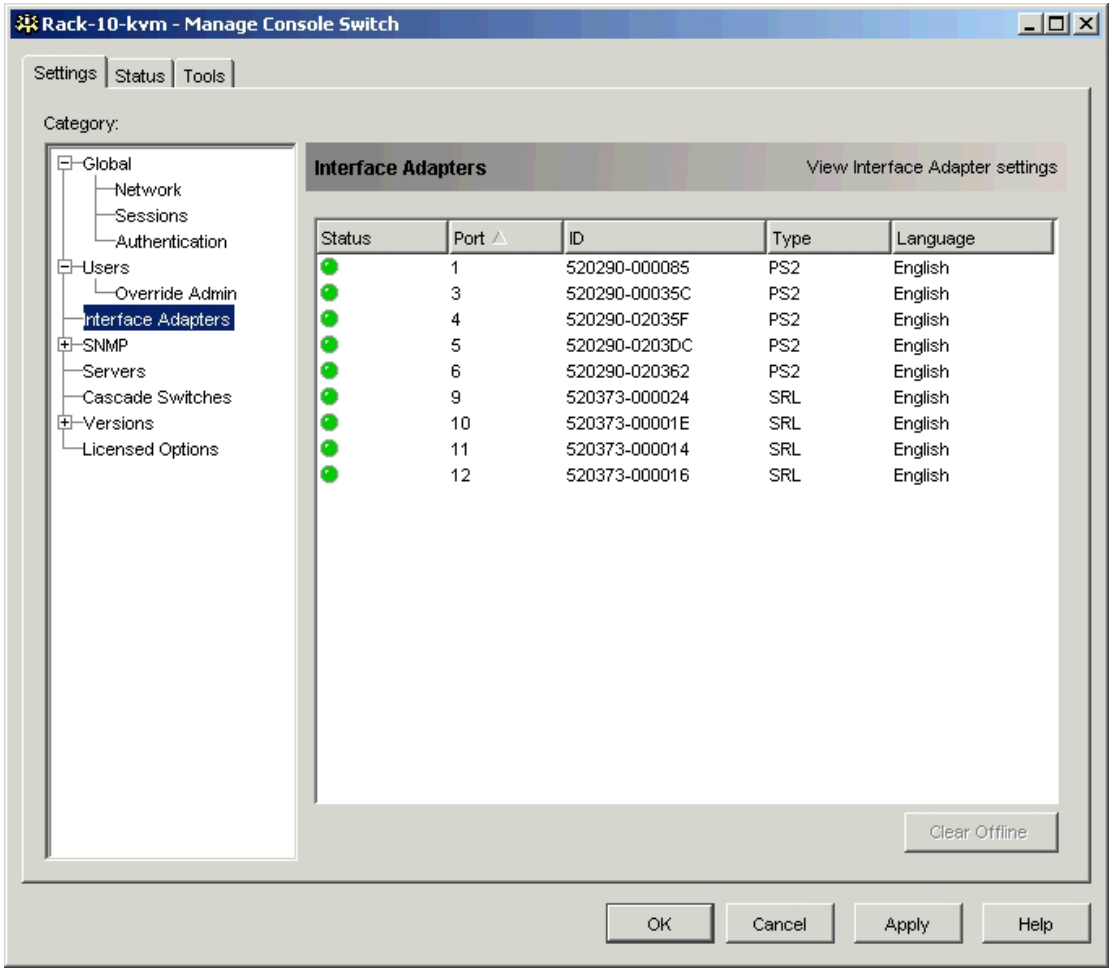

Figure 6-10: Interface Adapters category

Enabling and Configuring SNMP

SNMP is a protocol used to communicate management information between network management applications and console switches. Other SNMP managers can communicate with your console switch by accessing Management Information Base (MIB)-II and the public portion of the enterprise MIB. MIB-II is a standard MIB that many SNMP servers support.

When you select the SNMP category for the first time, the Manage Console Switch retrieves the SNMP parameters from the unit. The SNMP category enables you to enter system information and community strings, designate the management stations that can manage the console switch, and receive SNMP traps from the console switch. If you select Enable SNMP, the unit responds to SNMP requests over User Datagram Protocol (UDP) port 161. Port 161 is the standard UDP port used to send and retrieve SNMP messages.

NOTE: The Manage Console Switch uses SNMP within a secure tunnel to manage console switches. For this reason, UDP port 161 can be exposed on firewalls. You must expose UDP port 161 to monitor console switches through third-party SNMP-based management software.

Up to four allowable managers can be defined, and all IP addresses are defined as blank by default. If all four entries are left blank, all IP addresses are authorized to read and write to the HP IP Console Switch, provided that they have the correct SNMP community strings. If any of the SNMP allowable manager entries are not blank, then only the defined SNMP allowable managers have access.

The allowable managers setting does not affect whether the HP IP Console Viewer can view or manage the HP IP Console Switch.

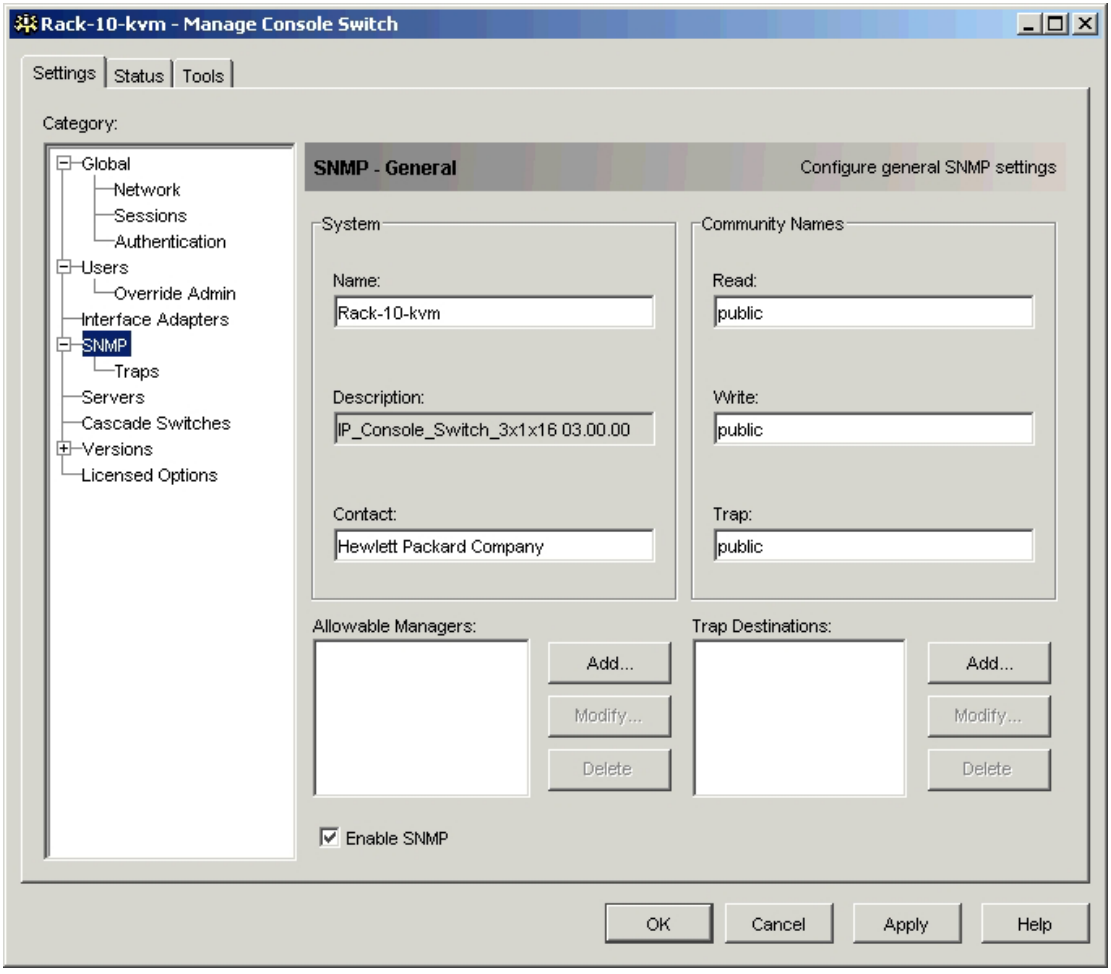

Figure 6-11: SNMP Category

Configuring General SNMP Settings

1. Select the SNMP category.
2. Select the **Enable SNMP** checkbox to configure the console switch to respond to SNMP requests over UDP port 161.
3. In the System section, enter the fully qualified domain name of the system in the Name field, a description in the Description field, and a contact person in the Contact field.

   IMPORTANT: If you are using LDAP or are planning to use LDAP in the future, the name in the Name field must match the computer name that represents the console switch in the active directory.

4. Enter the community names in the **Read** field, **Write** field, and **Trap** field. These specify the community strings that must be used in SNMP actions. The read and write strings only apply to SNMP over UDP port 161 and act as passwords that protect access to the console switch. The values can be up to 64 characters in length.
5. Add up to four SNMP management stations that are allowed to monitor the console switch, such as HP Systems Manager Insight, or leave the field blank to allow any SNMP management station to manage the HP IP Console Switch.

   NOTE: Adding an IP address to the Allowable Managers field does not prevent a user from managing the HP IP Console Switch with the HP IP Console Viewer.

   a. Click **Add** to define an allowable manager. The Allowable Manager dialog box appears.

   b. Enter the IP address of the SNMP management station that you want to add.

   c. Click **OK** to add an SNMP management station. The IP address appears in the Allowable Manager field.

6. Add up to four SNMP trap destinations to which this console switch sends traps in the Trap Destinations field.
   a. Click **Add** to define a trap destination. The Trap Destination dialog box appears.
   b. Enter the IP address of the trap destination you want to add.
   c. Click **OK** to add a trap destination. A reboot warning appears.
7. Click **OK** to save the settings and close the window.

   -or-

   Click **Apply** to save the settings and remain in the open window.

   -or-

   Click **Cancel** to exit the window without saving.

Enabling Individual SNMP Traps

An SNMP trap is a notification sent by the HP IP Console Switch to a management station to indicate that an unusual event has occurred in the switch that might demand further attention. You can specify what SNMP traps are sent to the management stations by deselecting or selecting the appropriate checkboxes in the list (the SNMP Authentication Failure Trap is not selected by default).

When you select the Traps category for the first time, the Manage Console Switch retrieves and displays a list of SNMP traps from the console switch. You can select Enable All or Disable All to easily select or deselect the entire list.

NOTE: The CPQKVM.MIB file is provided on the HP IP Console Viewer CD to be used with HP Systems Manager Insight or other SNMP management stations to properly receive SNMP traps.

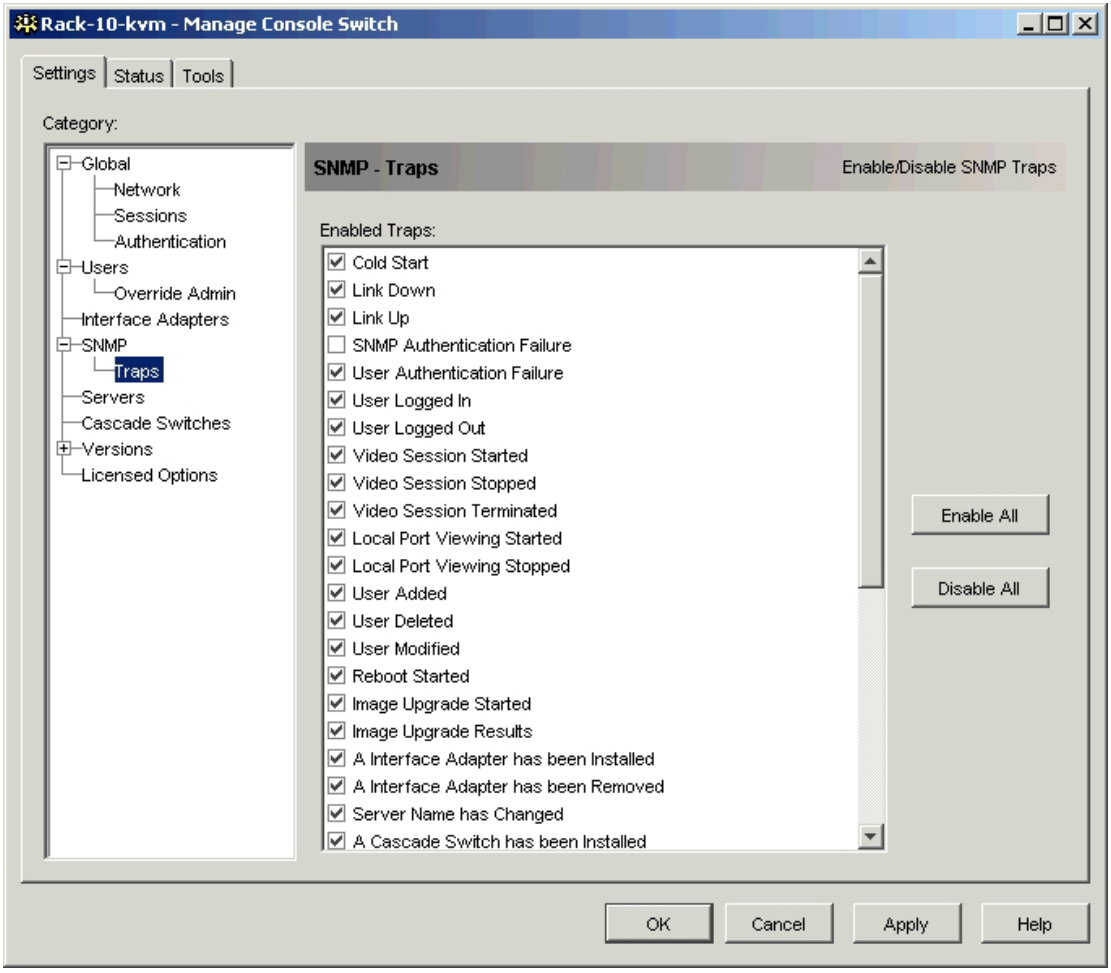

Figure 6-12: SNMP Traps subcategory

Viewing the Servers Category

When you select the Servers category for the first time, the Manage Console Switch retrieves the servers that exist in the HP IP Console Viewer database, as well as information on how the servers are connected to the selected console switch. The Servers category enables you to view the list of newly detected servers as well as update the HP IP Console Viewer database.

The Connections column displays the current server connection to either an Interface Adapter or a cascade switch. If the server is connected to an Interface Adapter, then the Interface Adapter ID displays in the connection column. If the server is connected to a cascade switch, the cascade switch and all its channels are displayed.

If you select either an Interface Adapter or a cascade switch in the Connections column, the Video Session Viewer appears.

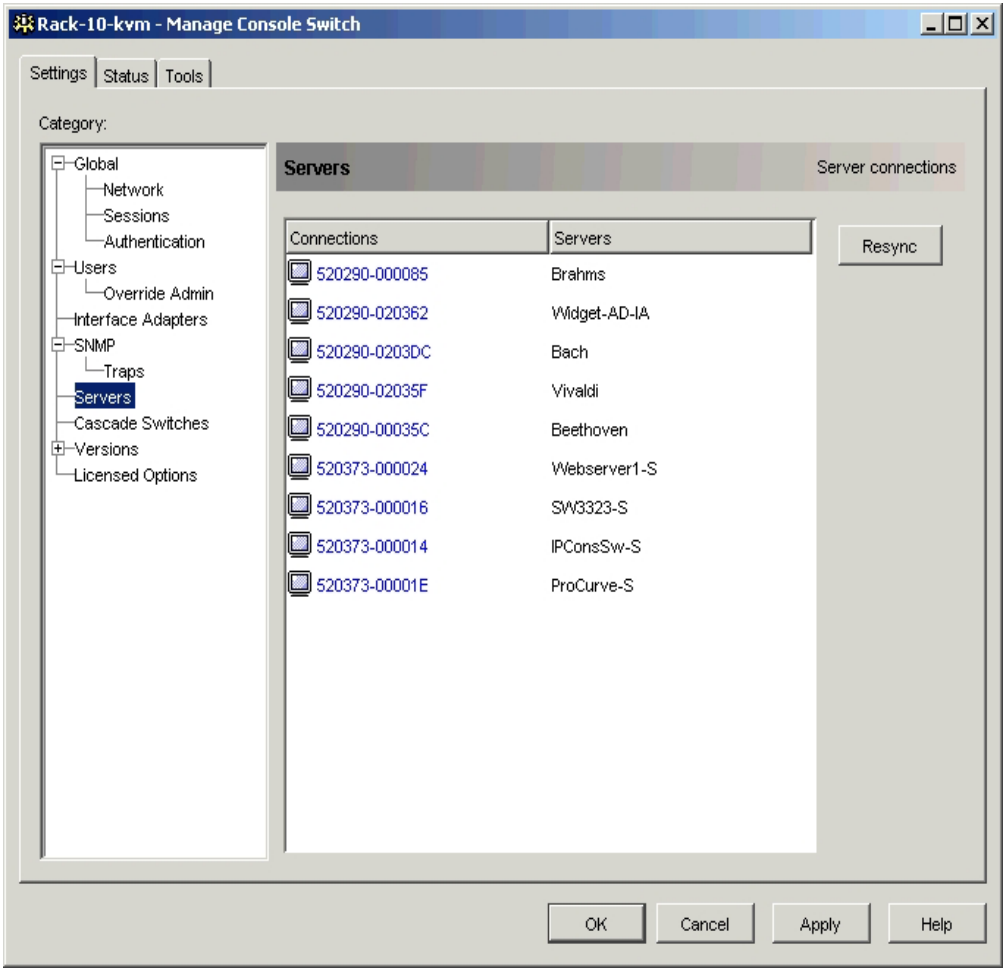

Figure 6-13: Servers category

Resyncing the Server Listing

You can choose to periodically resynchronize the database on the HP IP Console Viewer client with the database stored in the console switch. You can resync if the local analog workstation has changed server names or if Interface Adapters have been added or moved.

NOTE: This procedure only resynchronizes your HP IP Console Viewer client. If you maintain multiple HP IP Console Viewer clients, save your resynchronized local database, and load it into the other HP IP Console Viewer clients to ensure consistency.

1. Click **Resync.** The Welcome to the Resync Console Switch Wizard window appears.

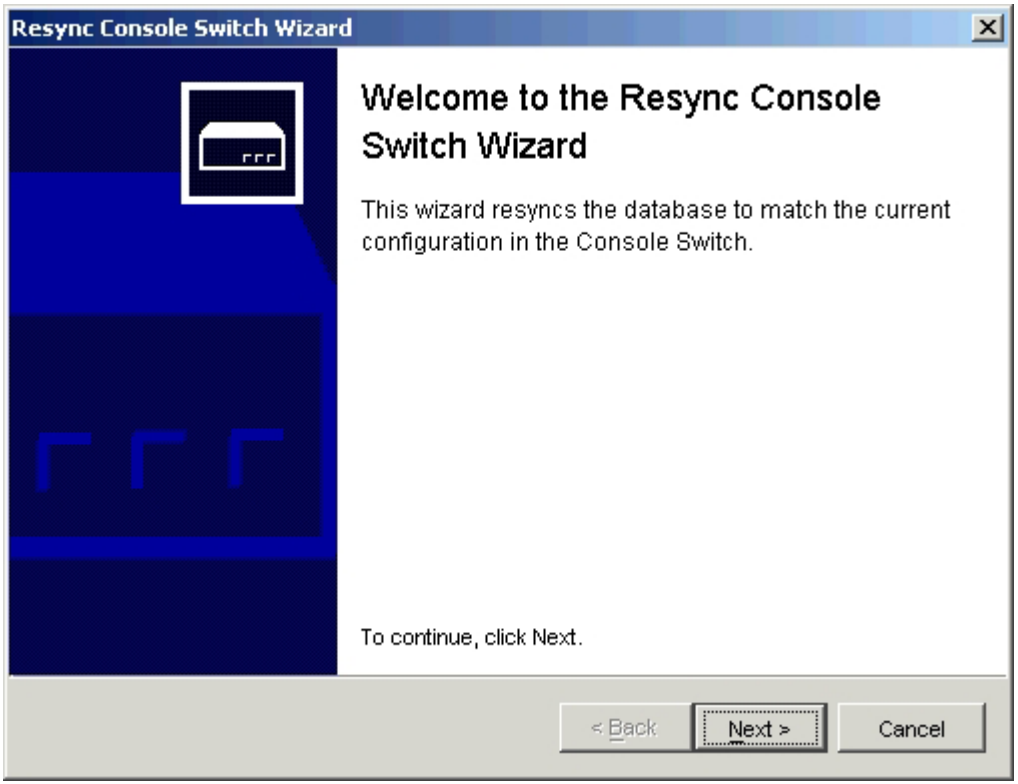

Figure 6-14: Resync Console Switch Wizard

2. Click **Next.** The Warning window appears.
3. (Optional) Select the **Include Offline Interface Adapters** checkbox for servers that are powered off.

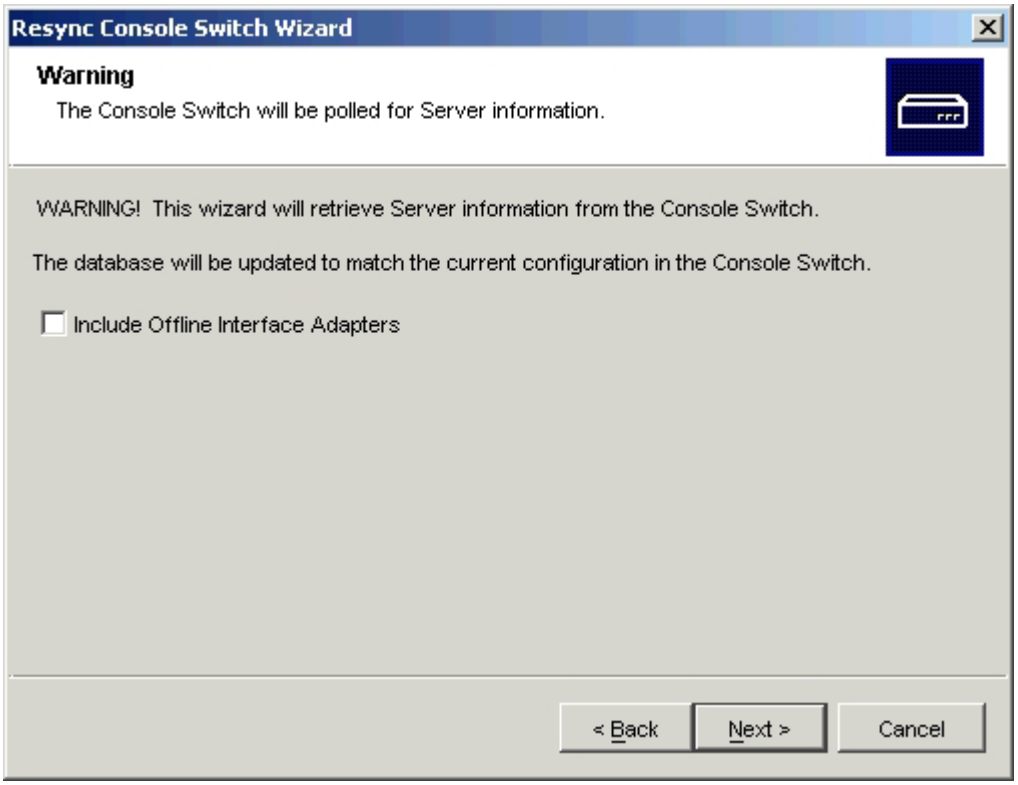

Figure 6-15: Warning window

4. Click **Next.** A progress bar appears, indicating that the console switch information is being reviewed.

   If no cascade switches attached to any Interface Adapters were detected, then the Completing the Resync Console Switch Wizard page appears. Click **Finish** to exit.

   -or-

   If any changes were detected, the Detected Changes window appears.

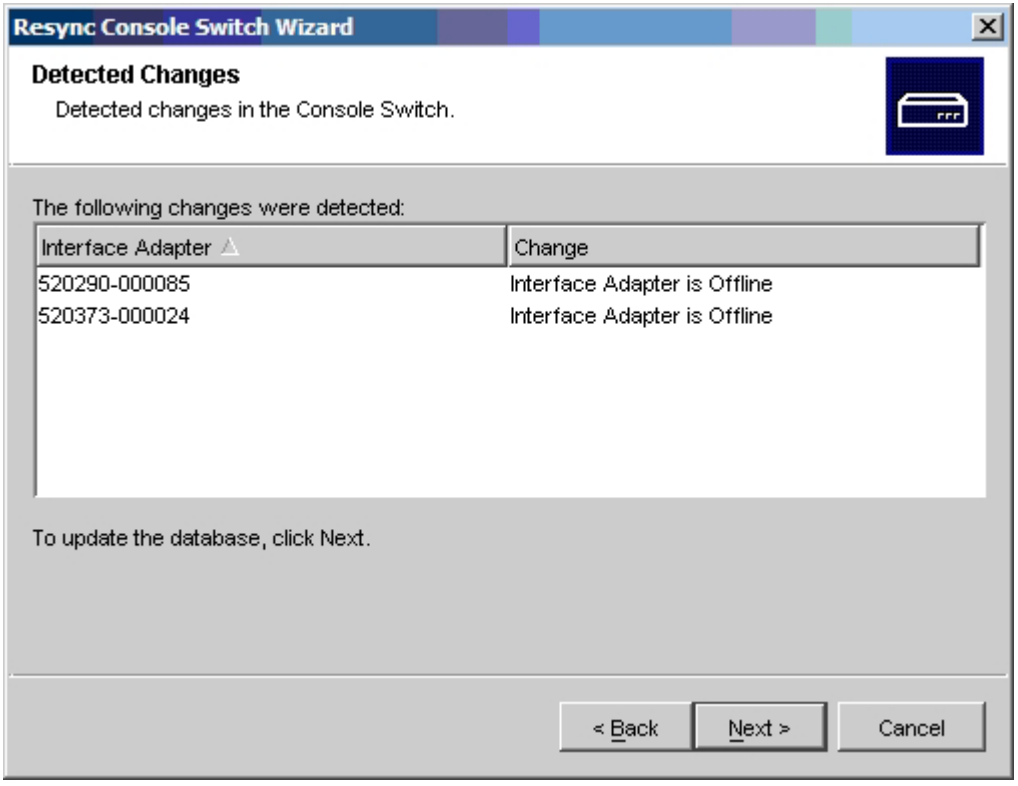

Figure 6-16: Detected Changes window

5. Click **Next** to update the database.

   If a cascade switch attached to at least one Interface Adapter is detected, then the Enter Cascade Switch Information window appears. Select the type of cascade switch connected to the console switch from the dropdown menu. If the type you are looking for is not available, you can add it by clicking **Add.** For more information, refer to the "Configuring Cascade Switch Connections" section in this chapter.

6. Click **Next.** The Completing the Resync Console Wizard window appears.

7. Click **Finish** to exit.

Configuring Cascade Switch Connections

The Cascade Switches category enables you to view, modify, and add cascade switch information into the HP IP Console Viewer database. The Assign Cascade Switch list only displays Interface Adapter IDs currently attached to a cascade switch in the database.

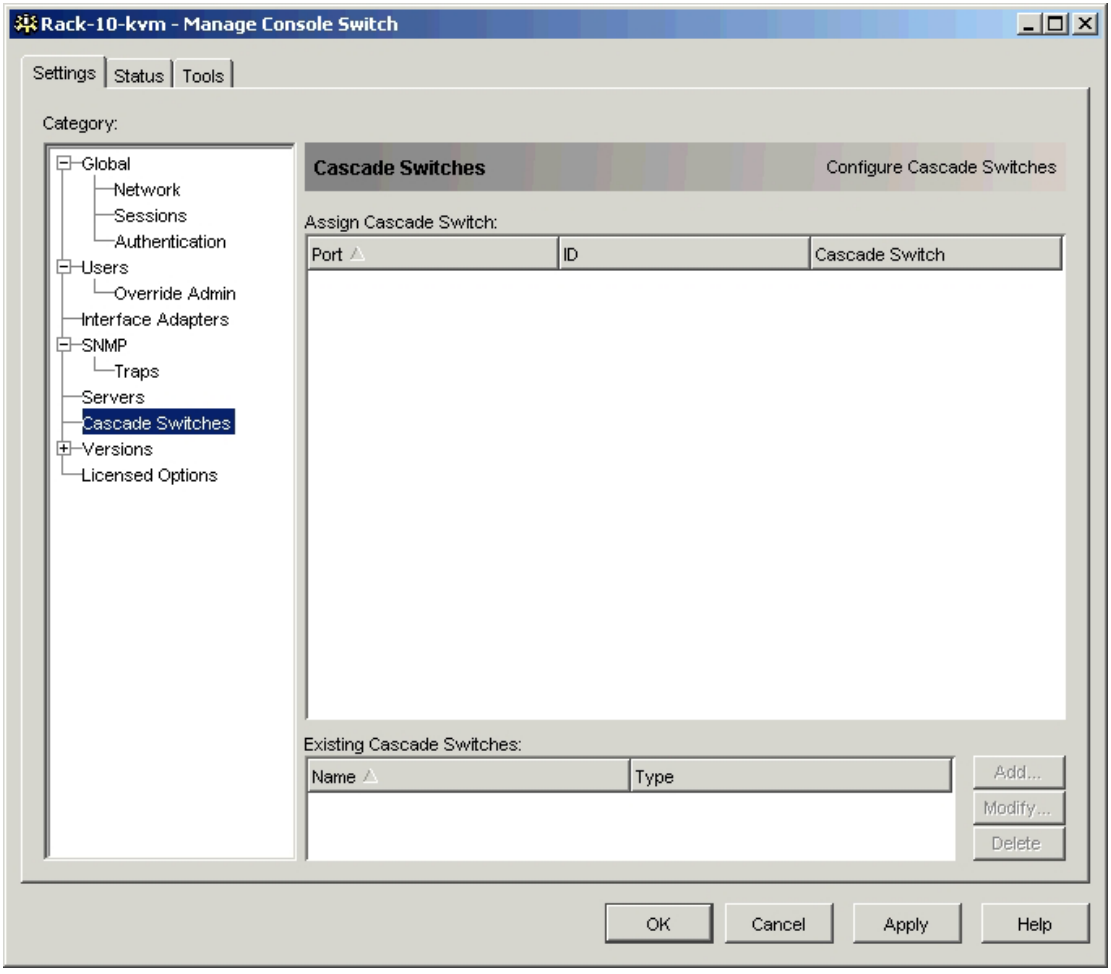

Figure 6-17: Cascade Switches category

To configure a cascade switch connection:

1. Select the **Cascade Switches** category.
2. Select the **Cascade Switch** dropdown list next to the ID column, select the cascade switch you want to configure, and select the console switch type you want to assign.

   -or-

   If the console switch is not in the dropdown list, add a console switch to the Existing Cascade Switches list by clicking **Add.** The Add Cascade Switch dialog box appears.

   a. Enter the name of the console switch, and select the console switch type from the list.

   b. Click **OK** to add the console switch. The console switch is now in the Existing Switches list and in the Cascade Switch dropdown list.
3. Repeat step 2 for each Interface Adapter.
4. When finished, click **Apply** and **OK** to save the new settings.

   -or-

   Click **Cancel.**

Loading Interface Adapter Firmware Individually

The Interface Adapter firmware can be loaded individually, from the Settings tab, or can be upgraded simultaneously, from the Tools tab. When a load is initiated, a message appears, indicating the current status. When a load is in progress, you cannot initiate another.

NOTE: This method of loading the Interface Adapter firmware will always overwrite the current version of firmware in the Interface Adapter. HP recommends using the Tools tab to upgrade your Interface Adapter firmware, which will only upgrade Interface Adapters needing a new version of firmware. For more information, refer to the "Using the Tools Tab" section in this chapter.

When you select the Versions category for the first time, the Manage Console Switch retrieves the firmware versions from the console switch itself. The Hardware subcategory displays the version information for the console switch itself. The Interface Adapter subcategory enables you to view and load all the Interface Adapters in the system.

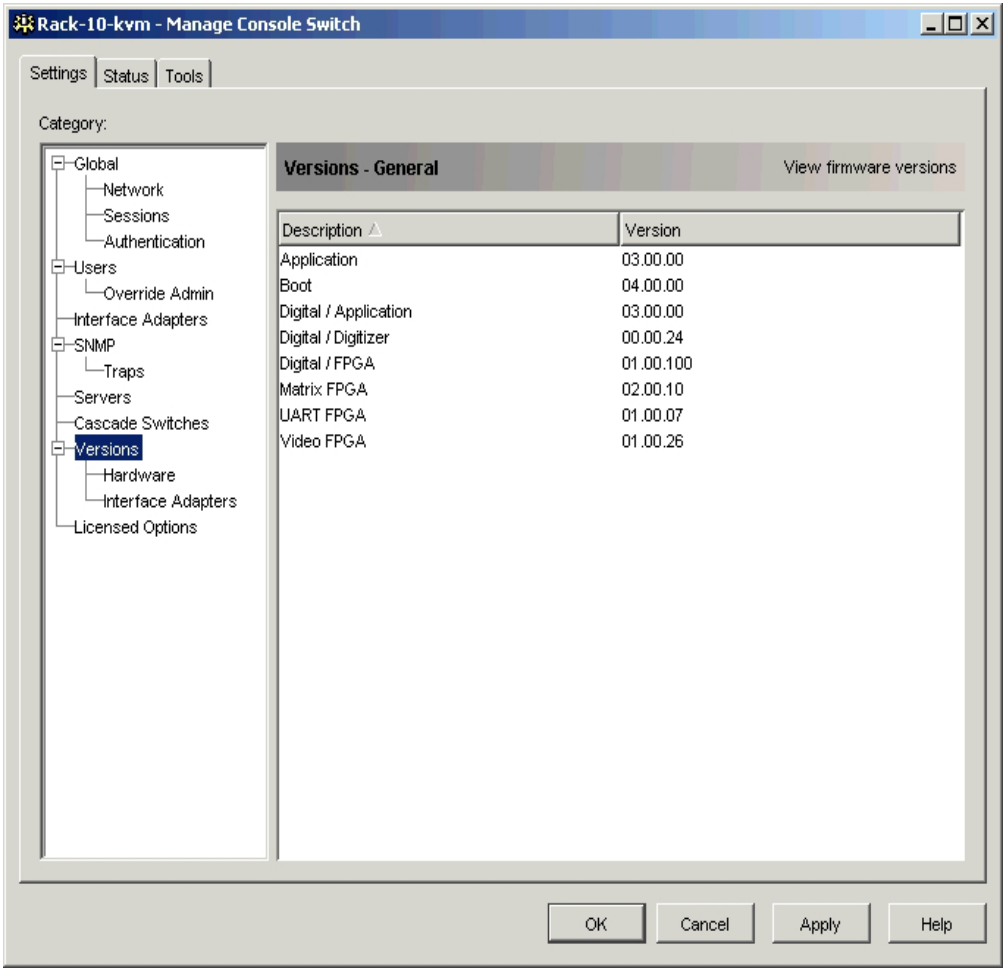

Figure 6-18: Versions category

Loading Individual Interface Adapter Firmware

1. Select the **Settings** tab in the Manage Console Switch.
2. Select **Versions>Interface Adapter.**

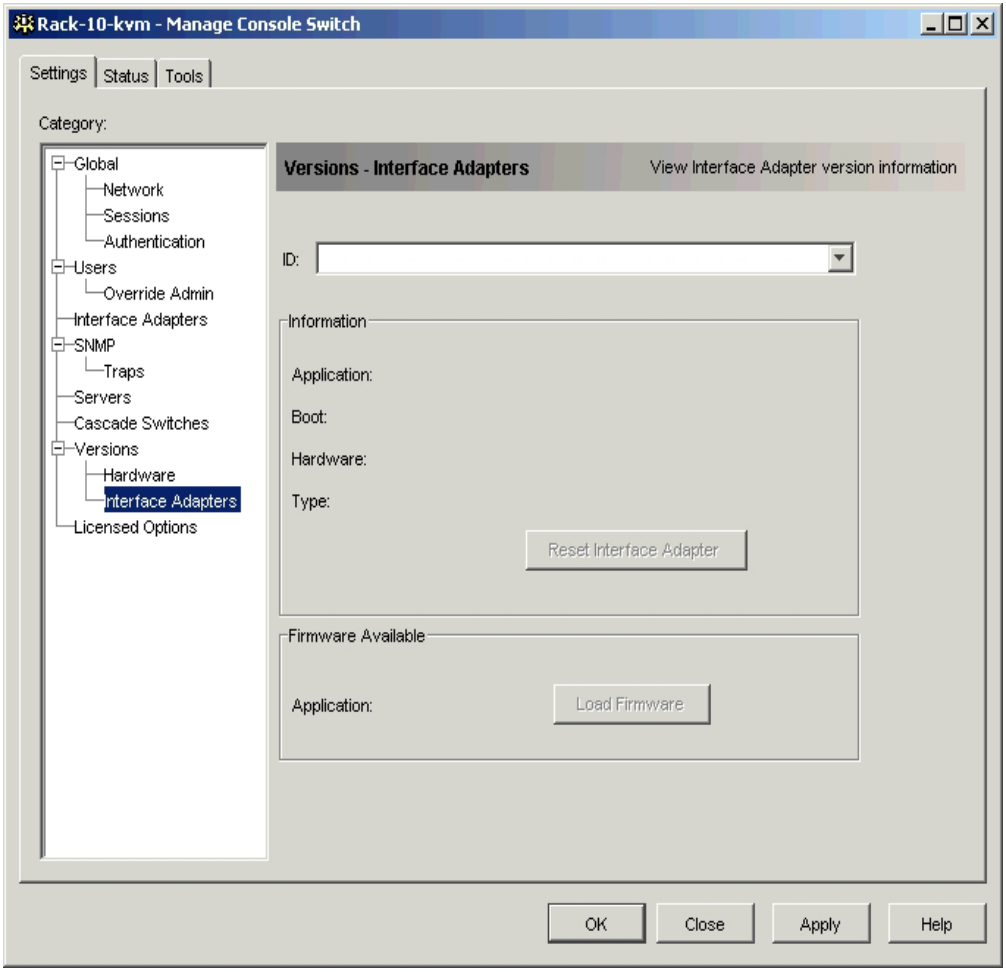

Figure 6-19: Interface Adapter Version subcategory

3. Select the **ID** dropdown list, and select the Interface Adapter for which you would like to view firmware information.

   The IDs displayed in the dropdown list are a combination of the IDs and either the server names or console switch names, depending on what is attached to the Interface Adapter. If the Interface Adapter is not attached to anything, the dropdown list displays None.

   After the Interface Adapter is selected, the firmware information appears in the Information box.

4. Compare the contents of the Information box to the Firmware Available box to see the firmware version available to the Interface Adapter. If the Interface Adapter requires upgrading, click **Load Firmware.** During the load process, the progress message appears below the Firmware Available dialog box and the Load Firmware button deactivates. When the load is complete, a message appears, confirming the upgrade.
5. Repeat steps 2 through 4 for each Interface Adapter to upgrade.
6. When finished, click **OK.**

Resetting an Interface Adapter

On occasions when a cascaded legacy console switch is not recognized by the console switch, it might be necessary to reset the Interface Adapter that connects the cascade switch to the console switch. To perform this action, use the Reset interface Adapter button in the Interface Adapter Version subcategory.

NOTE: The Reset Interface Adapter button is only enabled when the interface Adapter type is PS/2 and when a firmware upgrade is not in progress.

1. From the Interface Adapter subcategory, select the Interface Adapter you want to reset from the ID list.
2. Click **Reset Interface Adapter.** A message appears, warning you that this function is reserved for cascade switches and that resetting the Interface Adapter might result in the need to reboot the attached server.

Viewing Licensed Options

When you click **Licensed Options** in the Management Panel, the Licensed Options window appears and enables you to configure options for use that are available on the console switch firmware. The Licensed Options window lists each option available on the console switch and if the option has been enabled by a license key. For more information on Licensing Options, refer to Chapter 7 of this guide.

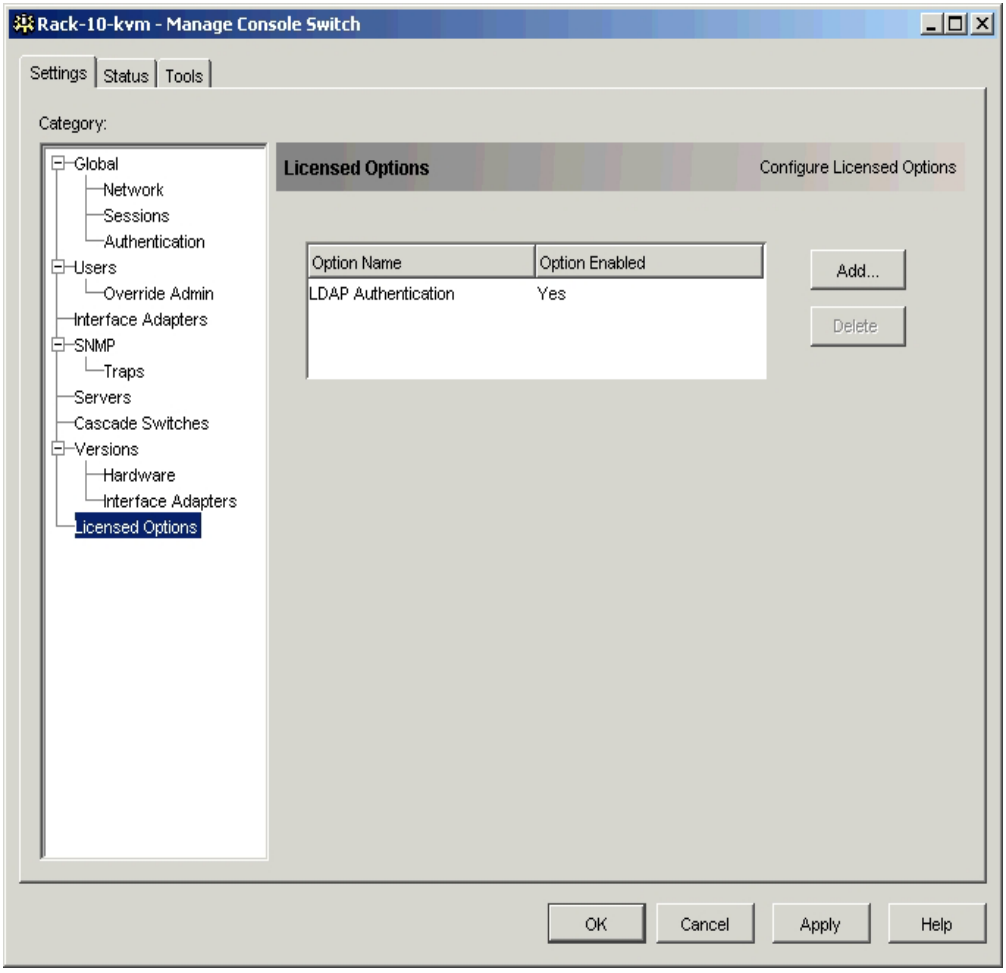

Figure 6-20: License Options category

Managing User Sessions

You can view and disconnect the current active user connections and unlock user accounts by using the Status tab in the Manage Console Switch. You can view the length of time users have been connected, the server names or Interface Adapter to which they are connected, and their system addresses.

Disconnecting User Session

1. Select the **Status** tab. The Currently active video sessions window appears.

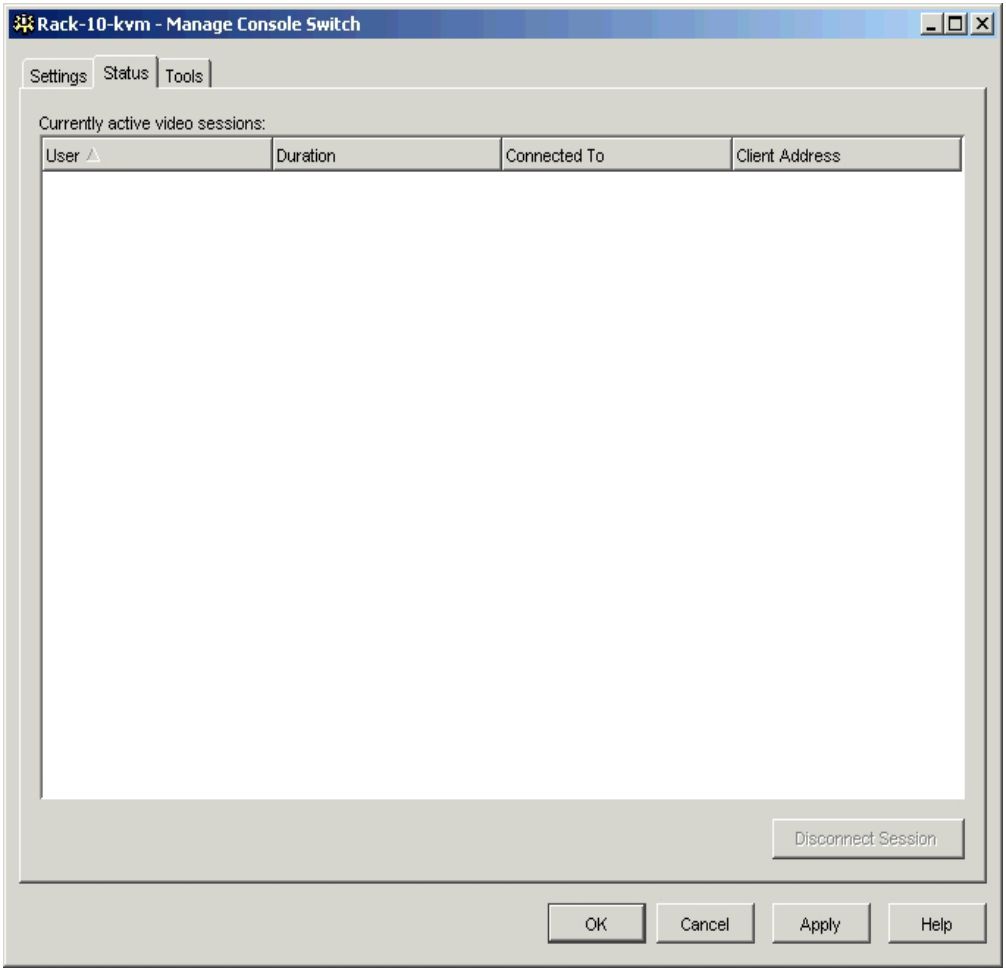

Figure 6-21: Currently active video sessions window

2. Select one or more users to disconnect.
3. Click **Disconnect Session.** The Confirm Disconnect dialog box appears.
4. Click **Yes** to confirm the disconnection.

   -or-

   Click **No** to exit without completing the disconnect command.

Using the Tools Tab

The Tools tab enables you to reboot, upgrade firmware, and save and restore both configuration and user database files.

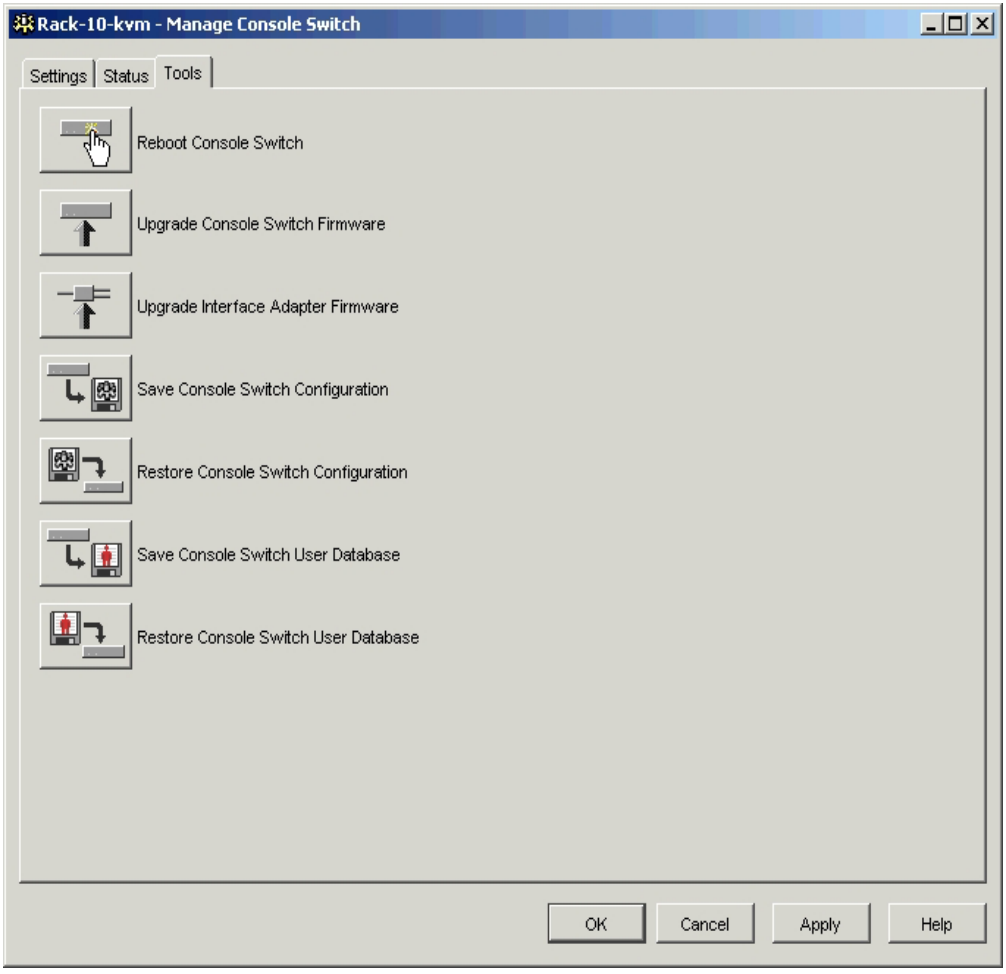

Figure 6-22: Tools tab

Rebooting the System

You can reboot the HP IP Console Switch using the Tools tab on the Manage Console Switch window. Clicking the **Reboot Console Switch** button causes the console switch to broadcast a disconnect message to any active users, then logs out the current user, and immediately reboots the console switch.

IMPORTANT: You must wait a minimum of 60 seconds after powering up to complete the boot cycle before performing any console switch operations. Attempting to access servers during the boot process might cause system errors that require a hardware reboot. Reboot the console switch, then wait 60 seconds after powering up before performing any console switch operations.

To reboot the console switch:

1. Select the **Tools** tab.
2. Click the **Reboot Console Switch** icon. A reboot warning appears.
3. Click **Yes.**

Upgrading Console Switch Firmware

You can upgrade the firmware for either the HP IP Console Switch or the Interface Adapter. The Interface Adapter can be upgraded individually, in the Settings tab, or simultaneously, in the Tools tab.

To perform Trivial File Transfer Protocol (TFTP) downloads, TFTP must be enabled. For more information, refer to Chapter 12 in this guide.

CAUTION: Do not power down the console switch while it is upgrading. This process can take up to 10 minutes to complete.

1. Select the **Tools** tab.
2. Click the **Upgrade Console Switch Firmware** icon. The Upgrade Console Switch Firmware dialog box appears. Enter the TFTP Server IP Address where the firmware is located, the firmware filename, and directory location.

NOTE: If you made changes in the Settings tab of the Manage Console Switch but have not yet applied those changes before starting the upgrade, a warning message prompts you to confirm the upgrade because the upgrade process requires that the console switch be rebooted. If you do not apply the changes, they are discarded before upgrading the firmware.

To apply the changes you have made before upgrading the console switch:

Click **No** to cancel the console switch firmware upgrade, and click **Apply.**

-or-

To discard the changes you have made before upgrading the console switch, click **Yes.**

Figure 6-23: Upgrade Console Switch Firmware dialog box

3. Click **Upgrade.** The Upgrade button deactivates, and a progress message appears. When the TFTP file transfer is complete, a message prompting you to confirm a reboot appears. The new firmware is not used until the console switch reboots.
4. Click **Yes** to reboot the console switch. The Upgrade Console Switch Firmware dialog box displays a progress message, eventually indicating that the upgrade and reboot are complete. Click **Close** to exit.

   -or-

   Click **No** to reboot at a later time.

Upgrading Interface Adapter Firmware Simultaneously

1. Select the **Tools** tab.
2. Click the **Upgrade Interface Adapter Firmware** icon. The Upgrade Interface Adapter Firmware dialog box appears.

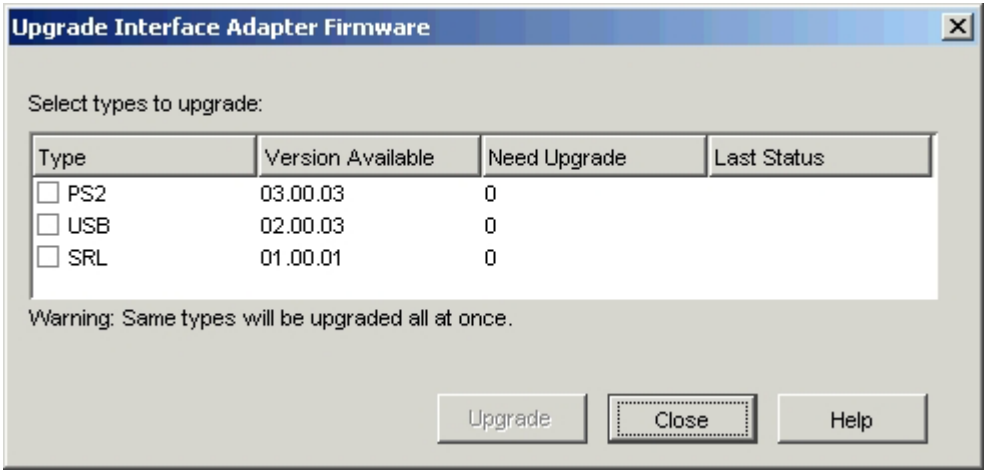

Figure 6-24: Upgrade Interface Adapter Firmware dialog box

3. Select the checkbox in front of the type of Interface Adapter you want to upgrade. The checkbox in front of the type cannot be selected if all the Interface Adapters have current firmware.
4. Click **Upgrade.** The Upgrade button deactivates. In the Last Status column, In Progress displays until the upgrade for that Interface Adapter type is complete, then Succeeded appears. A Firmware upgrade currently in progress message appears until all the selected Interface Adapters are upgraded.
5. Click **Close** to exit.

Managing Console Switch Configuration Files

Configuration files contain all the settings for a console switch, including network settings, Interface Adapter configurations, SNMP settings, and attached servers. Configuration files can also be written to new console switches, avoiding the requirement to manually configure a new console switch.

NOTE: User account information is stored in the user database, not in the configuration file (except for the Override Admin account, which is stored in the configuration file and not in the user database file). For more information, refer to the "Managing Console Switch User Databases" section in this chapter.

Saving Console Switch Configurations

1. Select the **Tools** tab.
2. Click the **Save Console Switch Configuration** icon. The Save HP IP Console Switch Configuration dialog box appears.
3. Click **Browse,** and select a location to save the configuration file. The location displays in the Filename: field.
4. Click **Save.** The Enter Password dialog appears.
5. Enter a password that will be used to encrypt the file and re-enter it in the Verify Password field. The configuration file is read from the console switch and saved to the desired location. A progress window appears.

   NOTE: Blank passwords are accepted, but not recommended.

6. When the save operation completes, a confirmation dialog is displayed. Click OK to return to the main window.

Restoring a Configuration File to a Console Switch

1. Select the **Tools** tab.
2. Click the **Restore Console Switch Configuration** icon. The Restore Console Switch Configuration dialog box appears.
3. Click **Browse,** and select the location of the saved configuration file. The file name and location are displayed in the Filename field.
4. Click **Open,** then click **Restore.** The Enter Password dialog appears.
5. Enter the password used when saving the file, and re-enter it in the Verify Password field to confirm.
6. When the restore operation completes, a confirmation dialog is displayed. Click OK to return to the main window.

Managing Console Switch User Databases

User database files contain all the user accounts assigned to a console switch, except for the Override Admin. You can save user account database files and use them to configure user accounts on multiple console switches by writing the user account file to the new console switch.

NOTE: You are prompted to enter a password that will be used to encrypt the file. It does not matter if you are restoring to a different unit or the same unit. The password is required to read (un-encrypt) the file to be restored.

Saving Console Switch User Databases

1. Select the **Tools** tab.
2. Click the **Save Console Switch User Database** icon. The Save Console Switch User Database dialog box appears.
3. Click **Browse,** and select a location to save the user database file. The location appears in the Filename: field.
4. Click **Save.** The Enter Password dialog appears.

5. Enter a password that will be used to encrypt the file and re-enter it in the Verify Password field. The configuration file is read from the console switch and saved to the desired location. A progress window appears.

   NOTE: Blank passwords are accepted, but not recommended.

6. When the save operation completes, a confirmation dialog is displayed. Click OK to return to the main window.

Restoring Console Switch User Databases

1. Select the **Tools** tab.
2. Click the **Restore Console Switch User Database** icon. The Restore Console Switch Database dialog box appears.
3. Click **Browse,** and select the location of the saved user database file. The file name and location are displayed in the Filename: field.
4. Click **Open,** then click **Restore.** The Enter Password dialog appears.
5. Enter the password used when saving the file, and re-enter it in the Verify Password field to confirm.
6. When the restore operation completes, a confirmation dialog is displayed. Click OK to return to the main window.

Changing Console Switch Properties

Individual console switch properties can be altered by selecting a console switch from the selected view. The Properties dialog box for console switches contains several tabs:

- **General**—Enables you to change the console switch name, console switch type, and console switch icon and assign the console switch a site, location, or folder
- **Network**—Enables you to change the IP address for that console switch
- **Information**—Enables you to enter information about the console switch, including a description, contact information, and any comments you might want to add

1. Select an individual console switch from the selected view.
2. Select **View>Properties** from the main menu.

   -or-

   Click **Properties.**

   -or-

   Right-click the console switch, and select **Properties** from the resulting list. The Properties dialog box appears.

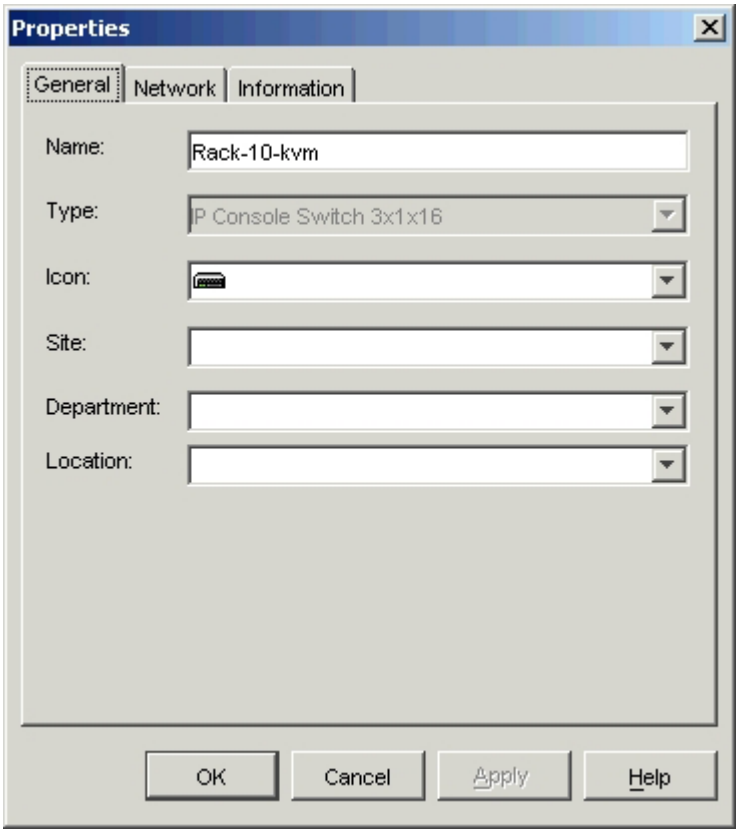

Figure 6-25: General tab

3. Enter the new name of the console switch. A warning appears if you enter a duplicate name.
4. Omit the **Type** field. This field is read-only for console switches.
5. Select the **Icon** to appear for the console switch.
6. (Optional) Select the Site, Department, and Location to which you would like the console switch assigned. If a selection is not in the dropdown list, enter the name of the new assignment in the text field. After it is entered, the option becomes available in the dropdown list for future assignment.

7. (Optional) Select the **Network** tab, and enter an IP address. This field can contain an IP dot notation or a domain name. Duplicate addresses are not allowed, and the field cannot be left blank. You can enter up to 128 characters.

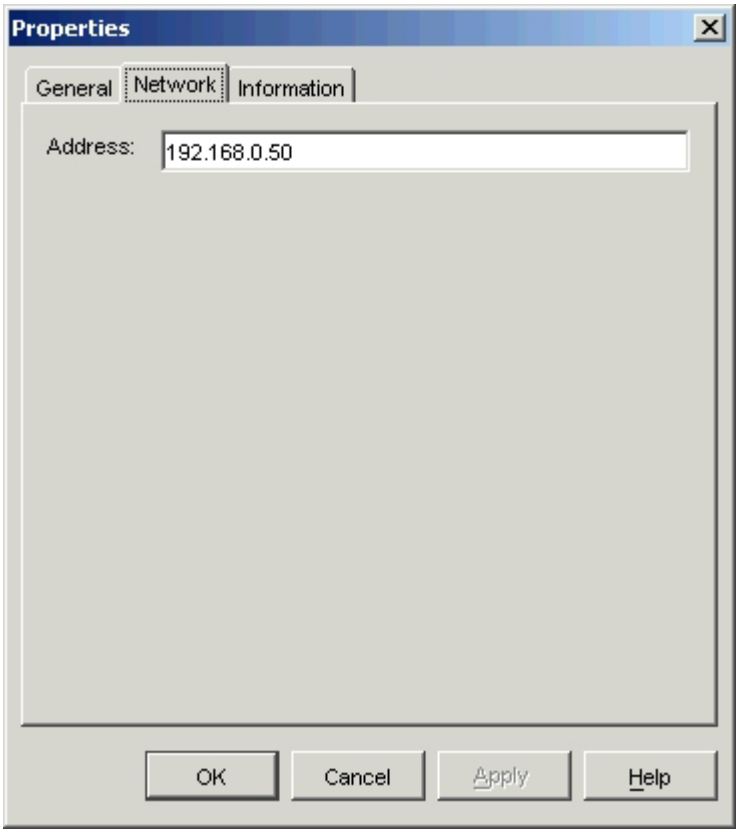

Figure 6-26: Network tab

8. (Optional) Select the **Information** tab, and enter the description of the console switch. You can enter any information into these fields.

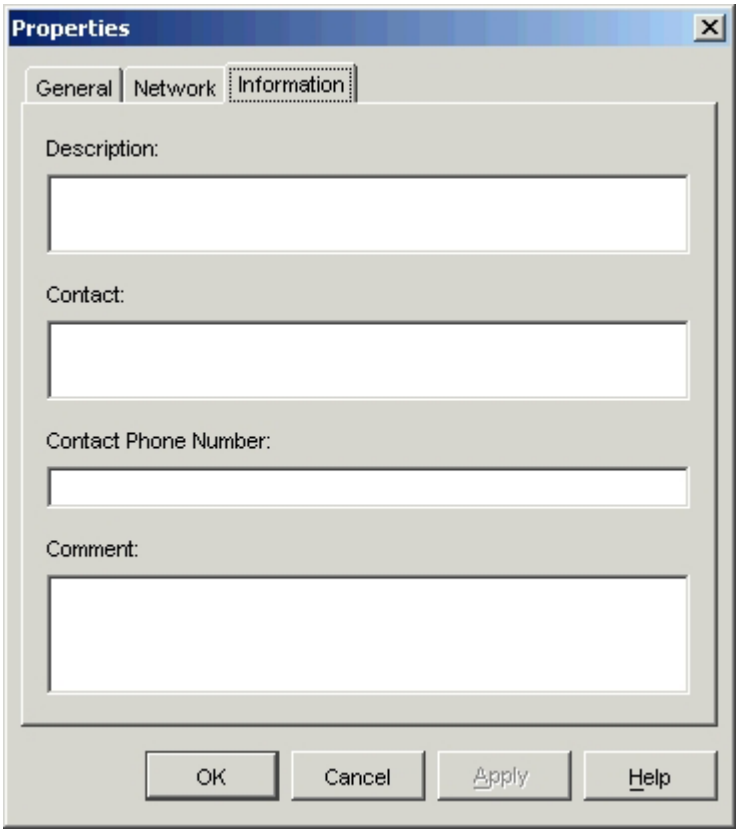

Figure 6-27: Information Tab

9. When finished, click **OK** to save the new settings, or click **Cancel** to exit without saving.

7

Using Directory Services Integration (LDAP)

You have two options for using Directory Services Integration:

- LDAP Authenticate only
- LDAP Authentication and Access Control

LDAP Authentication Only

In LDAP authentication only mode, the domain controller authenticates the user name and password, but access rights are still held on the console switch itself. So the console switch authorizes access. This solves the problem of ensuring secure passwords and removing users from the console switches as the authentication takes place within the directory.

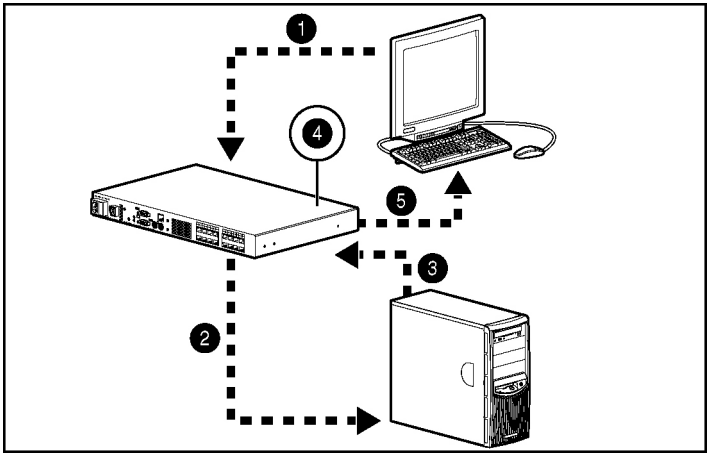

Figure 7-1: LDAP Authenticate Only mode

Item	Description
1	User sends request to console switch to access server.
2	Switch sends ID and password to domain controller.
3	Directory authenticates.
4	If authenticated, console switch authorizes access from its database.
5	If authorized, console switch allows console session for user.

LDAP Authentication and Access Control

In LDAP Authentication and Access Control mode, the domain controller authenticates and authorizes access.

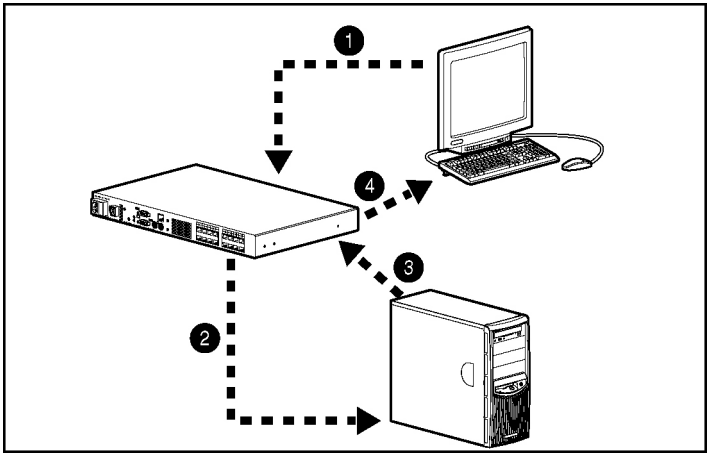

Figure 7-2: LDAP Authentication and Access Control Mode

Item	Description
1	User sends request to console switch to access server.
2	Console switch sends ID and password to domain controller.
3	Directory authenticates and authorizes.
4	If authenticated and authorized, console switch opens console session for user.

LDAP Authentication and Access Control Query Types

You can make two different types of requests:

- To administer the console switch
- To set up a remote console session with a server

In LDAP Authentication and Access Control mode, the console switch forwards these requests, or query types, to the domain controller.

Query Modes

The domain controller authenticates the user, but you determine how the domain controller handles authorization for each type of query. There are three authorization options:

- Basic mode
- User Attribute mode
- Group Attribute mode

LDAP Authentication and Access Control Basic Mode

In basic mode, if the domain controller authenticates the user, then it grants full access to the console switch or the server. HP recommends that the basic mode only be used for setup and testing and not in a production environment.

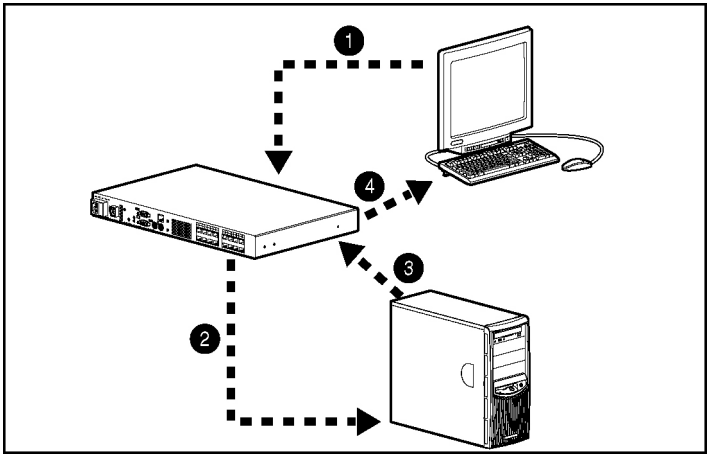

Figure 7-3: LDAP Authentication and Access Control Basic Mode

Item	Description
1	User sends request to console switch to access server.
2	Console switch sends ID and password to domain controller.
3	Directory authenticates and authorizes full access.
4	If authenticated and authorized, console switch opens console session for user.

LDAP Authentication and Access Control User Attribute Mode

In user attribute mode, if the domain controller authenticates the user, then it grants access to the console switch or the server based on the record of the user in the Active Directory. The record of the user contains an attribute. The attribute has access rights assigned to it.

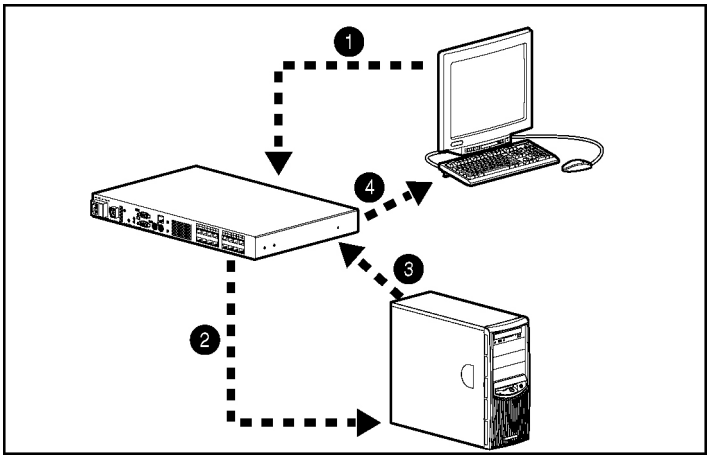

Figure 7-4: LDAP Authentication and Access Control User Attribute

Item	Description
1	User sends request to console switch to access server.
2	Console switch sends ID and password to domain controller.
3	Directory authenticates and authorizes based on rights assigned to attribute in user record.
4	If authenticated and authorized, console switch opens console session for user.

LDAP Authentication and Access Control Group Attribute Mode

In group attribute mode, if the domain controller authenticates the user, then it grants access to the console switch or the server based on the group that the user and the console switch, or server, are in. Access rights are set at the group level. If the user and the console switch, or server, are in the same group, then the group access rights determine what the user can do.

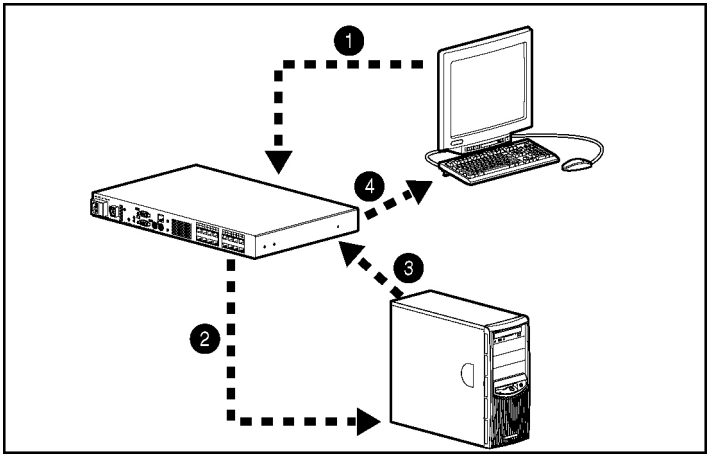

Figure 7-5: LDAP Authentication and Access Control Group Attribute

Item	Description
1	User sends request to console switch to access server.
2	Console switch sends ID and password to domain controller.
3	Directory authenticates and authorizes if user and console switch or server are in the same group.
4	If authenticated and authorized, console switch opens console session for user.

Purchasing License Keys

To purchase a license key, visit the HP website at http://h18004.www1.hp.com/products/servers/proliantstorage/rack-options/list.html#console.

-or-

Contact you nearest reseller.

Enabling Directory Services Integration

IMPORTANT: Before implementing Directory Services Integration functionality, refer to Appendix A for a better understanding of how Directory Services Integration works.

1. Access the console switch.
   a. Click the **Console Switches** icon to display the console switches in the selected view.
   b. Double-click the desired console switch.

      -or-

      Select the console switch, and click the **Manage Console Switch** icon.

      -or-

      Right-click the console switch, and click the **Manage Console Switch** icon from the resulting list.

      -or-

      Click the **Console Switches** icon, and press the **Enter** key.

      A login dialog box appears.
   c. Enter a valid user name and password. If a new user name and password have not been created, the default user name is `Admin` (case-sensitive) and the default password field is blank.

IMPORTANT: If you previously logged in to the console switch during the same HP IP Console Viewer session, the login dialog does not display.

d. Click **OK.** The Manage Console Switch window appears.

2. Select the **License Options** category.

   The Licensed Options window displays and enables you to configure options for use that are available on the console switch firmware. The Licensed Options window lists each option available on the console switch and if the option has been enabled by a license key.

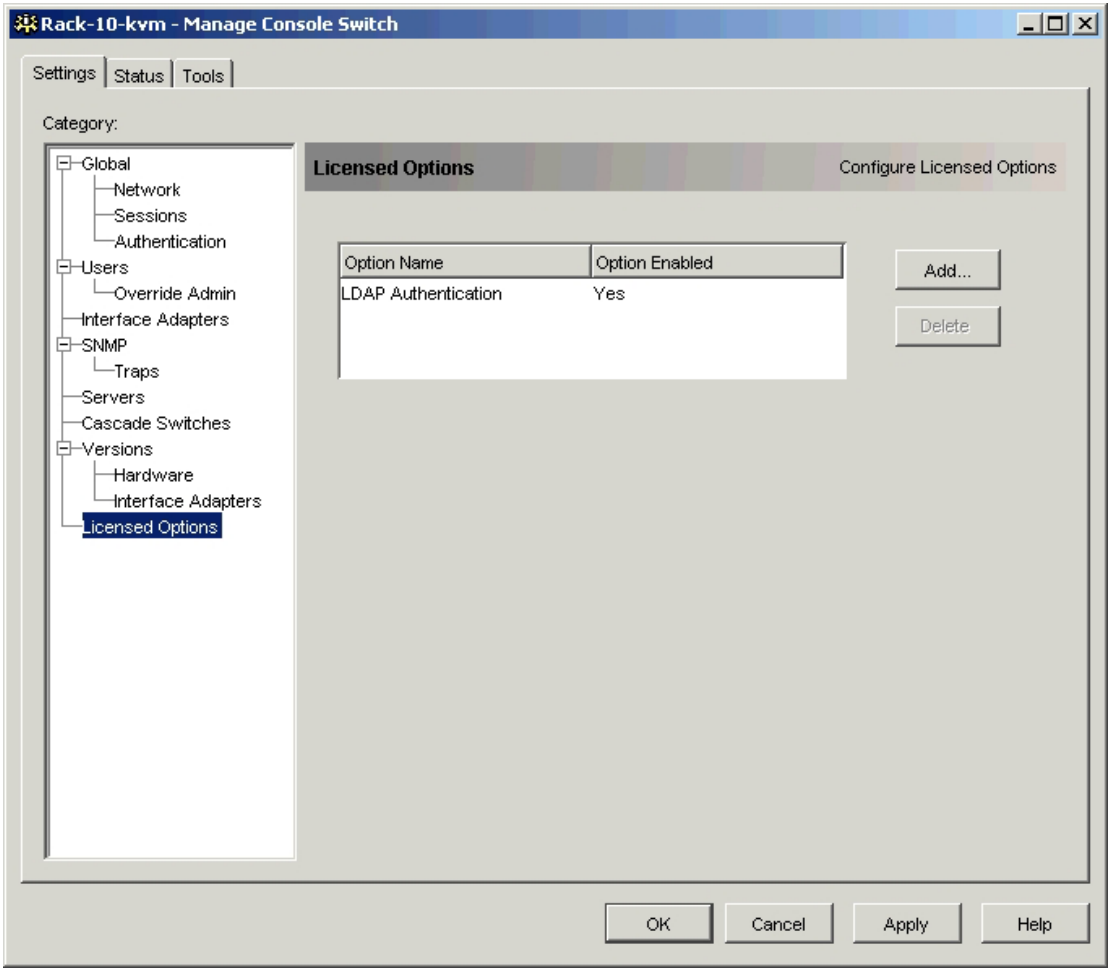

Figure 7-6: License Options category

3. Click the **Add** button on the right side of the window to enable the LDAP Authentication option. The Enter Key dialog box displays.

Figure 7-7: Enter Key dialog box

4. Enter a valid LDAP Authentication license key. The license key is composed of 25 case-sensitive characters.
5. Click **OK.** If the key is valid, the "LDAP Authentication" licensed option displays in the Option Name column and Yes displays in the Options Enabled column.

When the Authentication subcategory is selected, the Use LDAP Authentication setting becomes accessible, and the Authentication parameters are displayed but not accessible unless Use LDAP Authentication is selected.

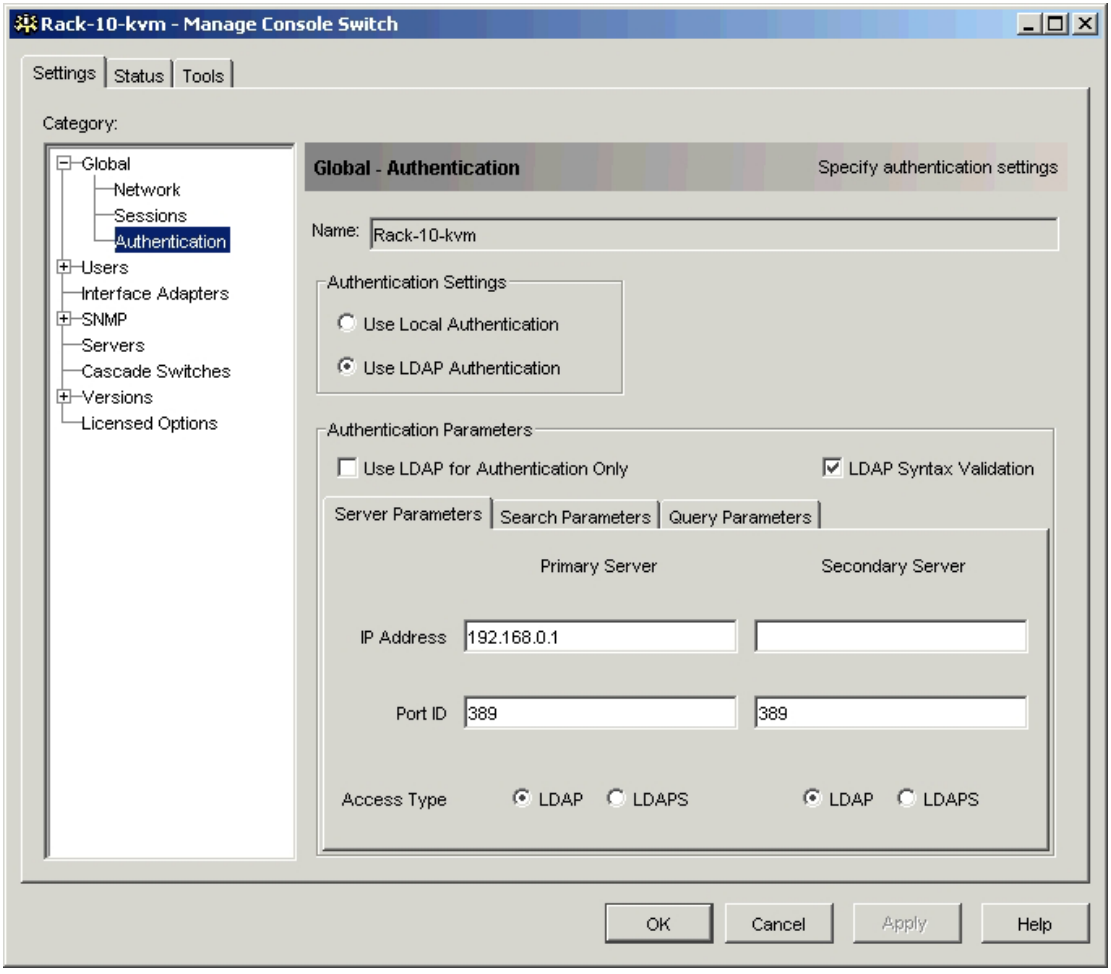

Figure 7-8: Authentication subcategory

6. To enable Local authentication and authorization, select the **Use Local Authentication** radio button. The Local method uses information from the Users subcategory to authenticate and authorize users attempting to manage the console switch or view an attached server.

   -or-

   To enable LDAP authentication and authorization, select the **Use LDAP Authentication** radio button. The LDAP method uses information from the LDAP Directory Service to authentication and authorize users attempting to either manage the console switch or view an attached server.

7. If Use LDAP Authentication is selected, then by default both authentication and authorization are controlled by information stored in the LDAP Directory Service. However, it is possible to specify that only authentication is to be controlled by the LDAP Directory Service, while authorization is to be controlled by information in the Users category. Select the **Use LDAP for Authentication Only** checkbox if authentication is to be controlled by the LDAP Directory Service and authorization is to be controlled by information in the Users subcategory.

Configuring LDAP Parameters

NOTE: There are differences between the LDAP-based access controls used by keyboard, video, and mouse (KVM) console switches and Kerberos-based access control that Windows uses by default when users log in to workstations and servers. Some of the user account properties in Active Directory apply only to Kerberos, while some apply to both Kerberos and the LDAP-based access controls used by KVM console switches. For example, configurable user restrictions, like the "Log On To," "Logon Hours," and "Managed By" features, in Active Directory do not apply to KVM console switches and their attached servers. Other features, like user account expiration, user account lockout, and the capability to disable a user account, do apply to KVM console switches and attached servers (subject to configuration of associated parameters in Active Directory). Because of the complexity of Active Directory, it is always useful to run test cases to confirm it is correctly configured to enforce the desired security policy. It is important to remember that LDAP is not capable of accessing the ACL data used by Windows to make its access control decisions. HP recommends following the configuration guidance provided by this software guide. Configurations outside that guidance are not supported.

If individual user accounts are stored on an LDAP-enabled directory server, such as Active Directory, you can use the Directory Service to authenticate users.

The settings made in the Authentication subcategory enable you to configure your authentication configuration parameters. The HP IP Console Viewer sends the user name, password, and other information to the console switch, which then determines whether the HP IP Console Viewer user has permission to view or change configuration parameters for the console switch in the HP IP Console Viewer main window.

CAUTION: Unless otherwise specified, use the LDAP default values unless Active Directory has been reconfigured. Modifying the default values might cause LDAP server communication errors.

There are three tabs for configuring LDAP parameters.

Server Parameters Tab

The Server Parameters tab displays the parameters that define LDAP server connection information.

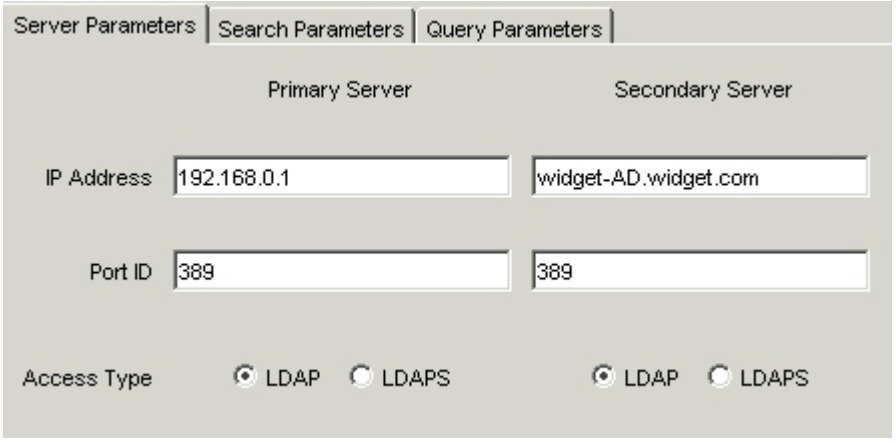

Figure 7-9: Server Parameter tab

Enter the primary and secondary server IP address in the IP Address fields. Each address may be entered in numeric form or by specifying a symbolic name that is registered in the DNS Service specified in the Network subcategory.

NOTE: Entering information into the Secondary Server IP Address field is optional.

Enter the UDP port numbers that are used to communicate with the LDAP servers in the Port ID fields. The default value is 389 for non-secure LDAP and 636 for secure LDAP. The HP IP Console Viewer automatically enters the Port ID when an Access Type is specified.

Specify how a query is sent to each LDAP server by selecting the appropriate Access Type radio button. Selecting the LDAP radio button sends plain text, while the LDAPS radio button sends LDAP over SSL.

NOTE: When the LDAP radio button is selected, all user names, passwords, and so on sent between a console switch and an LDAP server are sent as non-secure plain text. For secure, encrypted communication between a console switch and the LDAP server, select the **LDAPS** radio button.

NOTE: LDAPS is only valid if the directory server is configured for LDAPS.

Search Parameters Tab

The Search Parameters tab displays the parameters used when searching the LDAP Directory Service to find user accounts and accounts that represent servers that are attached to console switches.

NOTE: The information in the Search DN and Search Base fields for dc=parameters must match. For example, in the Search DN field if you have dc=widget, in the Search Base field, the dc=parameters must also say dc=widget.

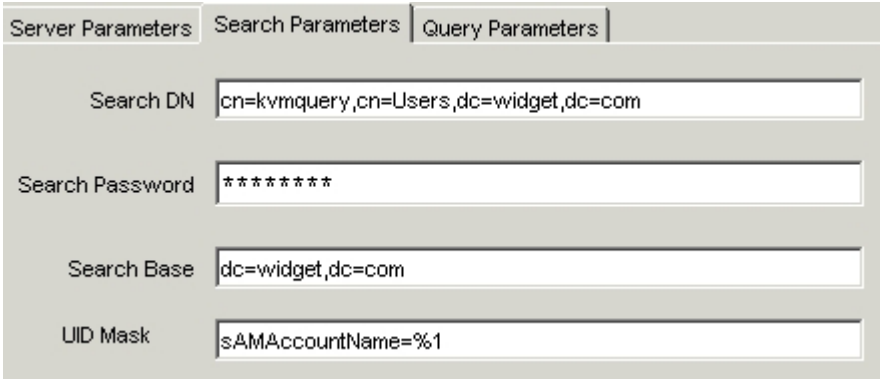

Figure 7-10: Search Parameters tab

The Search DN field enables you to define any user in the directory that the console switch uses to log in to the Directory Service.

NOTE: HP recommends creating a user account specifically for LDAP queries instead of using the admin account.

After the console switch is authenticated, the Directory Service grants it access to the directory to perform the user authentication queries specified on the Query Parameters tab. The default values are cn=Administrator, cn=Users, dc=yourDomainName, and dc=com and should be modified for your network environment. For example, to define an administrator Distinguished Name (DN) for test.view.com, enter cn=Administrator, cn=Users, dc=test, dc=view, dc=com. This is a required field unless the Directory Service has been configured to allow anonymous search, which is not the default.

NOTE: A comma must separate each Search DN value.

The Search Password field is used to authenticate the administrator or user specified in the Search DN field.

The Search Base field enables you to define a starting point from which LDAP searches begins. The default values are dc=yourDomainName, and dc=com, and should be modified for your network environment. HP recommends that the Search Base field be set to the DN of the root of the LDAP Directory Service namespace. For example, to define a search base for test.com, enter dc=test, dc=com.

NOTE: A comma must separate each Search Base value.

The UID Mask field specifies the search criteria for User ID searches of LDAP servers. The format should be in the form <name>=<%1>, where <name> is the display name in the directory. The default value is sAMAccountName=**%1**, which is correct for use with Active Directory. This field is required for LDAP searches.

Query Parameters Tab

NOTE: When the Use LDAP for Authentication Only checkbox is selected, all of the Query Parameters tab fields are deactivated.

The Query Parameters tab specifies which query method is used to authenticate and authorize the user. It also specifies the parameters associated with each query method.

The console switch performs two different types of queries. Query Mode (Console Switch) is used to authenticate administrators attempting to access the console switch itself. Query Mode (Server) is used to authenticate users who are attempting to access attached servers.

Additionally, each type of query has three modes that utilize certain types of information to determine whether or not a user has access to a console switch and/or connected servers.

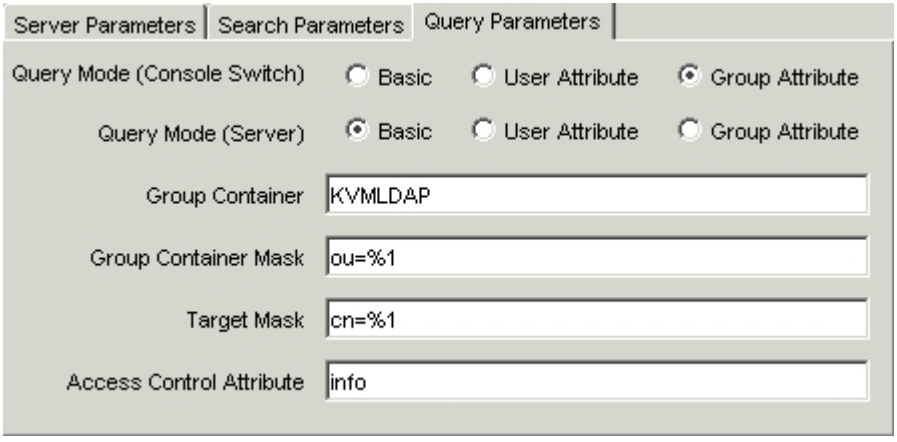

Figure 7-11: Query Parameters tab

The Query Mode (Console Switch) parameters are used to determine whether an HP IP Console Viewer user has Console Switch Administrator or Administrator access to the console switch.

The Query Mode (Server) parameters are used to determine whether a user of the HP IP Console Viewer application has user access to servers attached to a console switch. The Query Mode (Server) cannot be used to grant Console Switch Administrator access to a console switch.

The Group Container, Group Container Mask, and Target Mask fields are only used for Group Attribute query modes and are required when performing a Console Switch or Server Group Attribute query.

The Group Container field specifies the organizational unit (OU) created in the Active Directory by the administrator as the location for group objects. Group Container is used when Query Mode is set to Group Attribute. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, console switches, and target devices). Setting the value of an attribute in the group object configures the access level associated with a group. For example, if the Notes property in the group object is used to implement the access control attribute, the Access Control Attribute field in the Query Parameters tab should be set to info. Setting the Notes property to *KVM Appliance Admin* causes the members of that group to have administration access to the console switches, and access to target devices that are also members of that same group. Setting the Notes properly to KVM User causes the members of that group to have access to any target devices in the group.

The Group Container Mask field defines the object type of the Group Container, which is normally an organizational unit. The default value is ou=%1.

The Target Mask field defines a search filter for the server. The default value is cn=%1.

The Access Control Attribute field specifies the name of the attribute that is used in Attribute query modes. The default value is info.

NOTE: The value of the Notes property available in group and user objects shown in Active Directory User and Computers is stored internally in the directory, in the value of the info attribute.

Console Switch and Server Query Modes

One of three different modes might each be used for Query Mode (Console Switch) and Query Mode (Server):

- **Basic**—A user name and password query for the HP IP Console Viewer user is made to the Directory Service. If they are verified, the HP IP Console Viewer user is given administrator access to the console switch and any connected devices for Query Mode (Console Switch) or to any selected device for Query Mode (Server).

  IMPORTANT: This mode enables any user that is in the Active Directory to have full access. This mode is valuable for testing. However, for production, HP recommends that you change this mode.

- **User Attribute**—A user name, password, and Access Control Attribute query for the console switch user is made to the Directory Service. The Access Control Attribute is read from the user object in the Active Directory.

  If the value *KVM Appliance Admin* is found, the HP IP Console Viewer user is given administrator access to the console switch and any connected servers for Query Mode (Console Switch) or to any devices for Query Mode (Server).

  If the value *KVM User* is found, then the HP IP Console Viewer user is given access to the server.

  The following are examples showing how the Admin and Console Switch User attribute modes are defined in Active Directory for a user named Charlie.

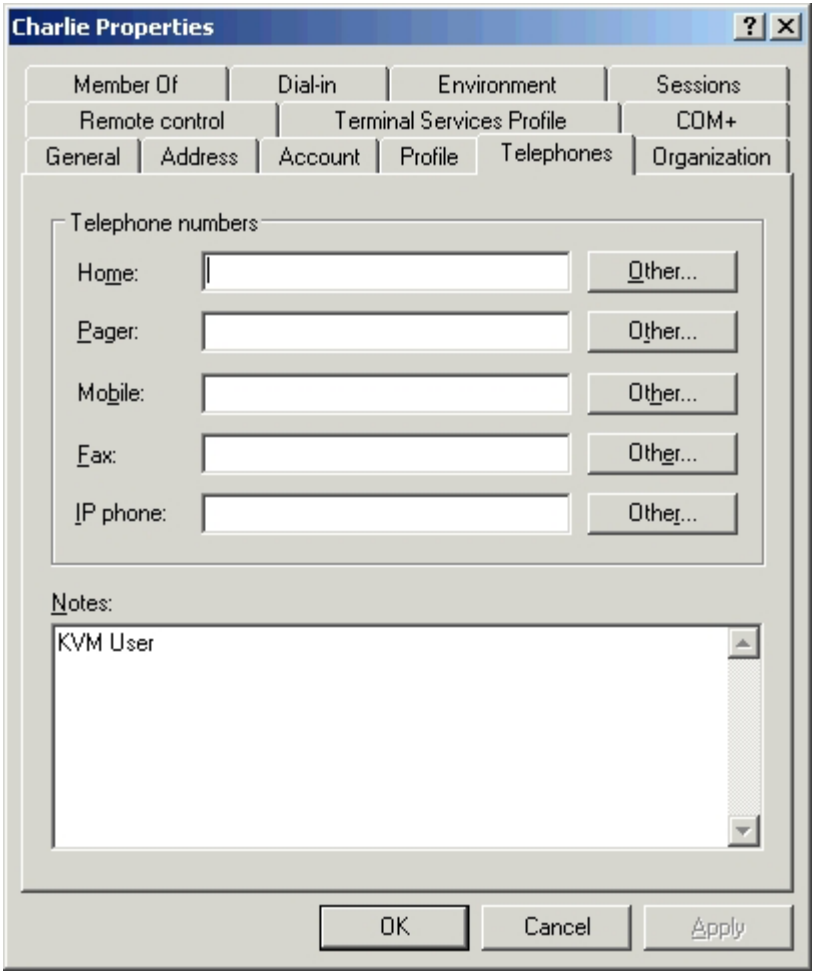

Figure 7-12: *KVM User* Attribute for User *Charlie*

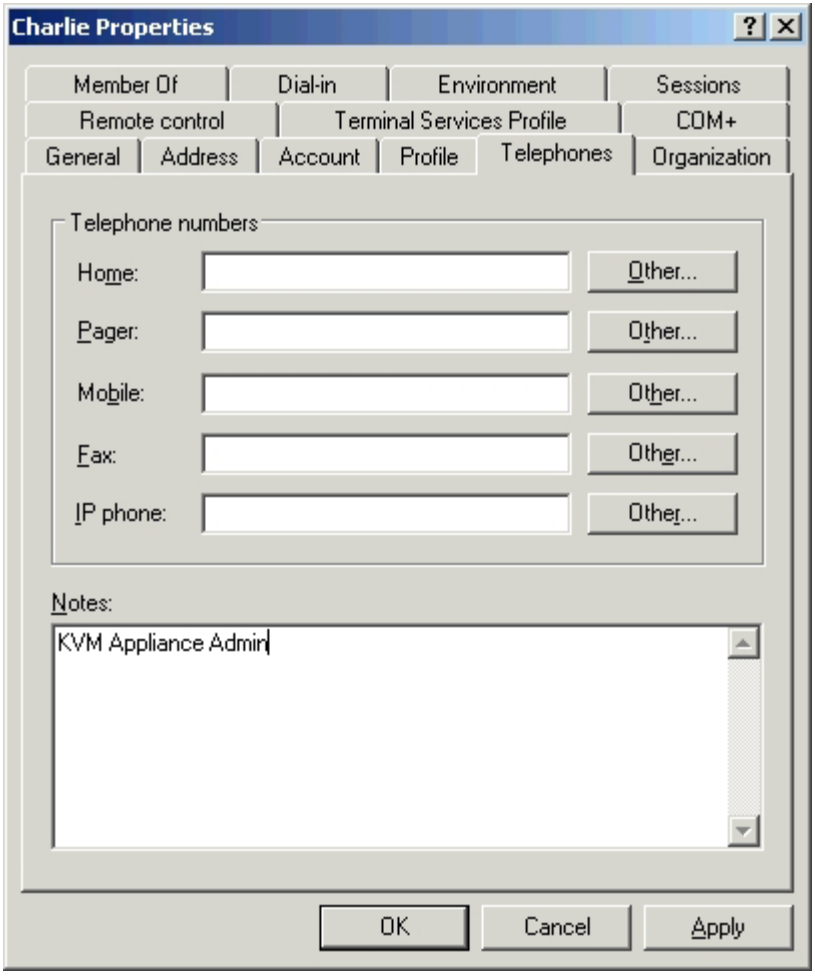

Figure 7-13: *KVM Appliance Admin* Attribute for *Charlie*

- **Group Attribute**—A user name, password, and group attribute query is made to the LDAP Directory Service for a console switch when using Query Mode (Console Switch) or for all devices when using Query Mode (Server). If a group is found containing the user and the console switch name, the HP IP Console Switch user is given user access to the console switch, connected servers, or both, depending on the group contents, when using Query Mode (Console Switch). If a group is found containing the user and server IDs, the user is given user access to the specified servers connected to the console switch when using Query Mode (Server).

  If the value *KVM Appliance Admin* is found, the HP IP Console Viewer user is given administrator access to the console switch and any connected servers for Query Mode (Console Switch) or to any devices for Query Mode (Server).

  If the value *KVM User* is found, then the HP IP Console Viewer user is given access to the server.

  Groups can be nested to a maximum of 16 levels in depth. Nesting enables you to have groups within other groups. For example, you might have a top-level group named Computers that contains a member named R&D, which is a group. The R&D group might contain a member named Domestic, which is a group, and so on.

  NOTE: Nesting to the maximum depth of 16 levels might not always be possible because of potential complexities among the nested groups. For example, if the nested groups are in different LDAP servers, then delays might occur when searching for all members of the nesting. These delays can cause the HP IP Console Viewer application to be unable to resolve the membership of a nesting in a reasonable amount of time.

  IMPORTANT: Before implementing LDAP functionality, refer to Appendix A for a better understanding of how LDAP works.

  The following are examples of groups defined in Active Directory.

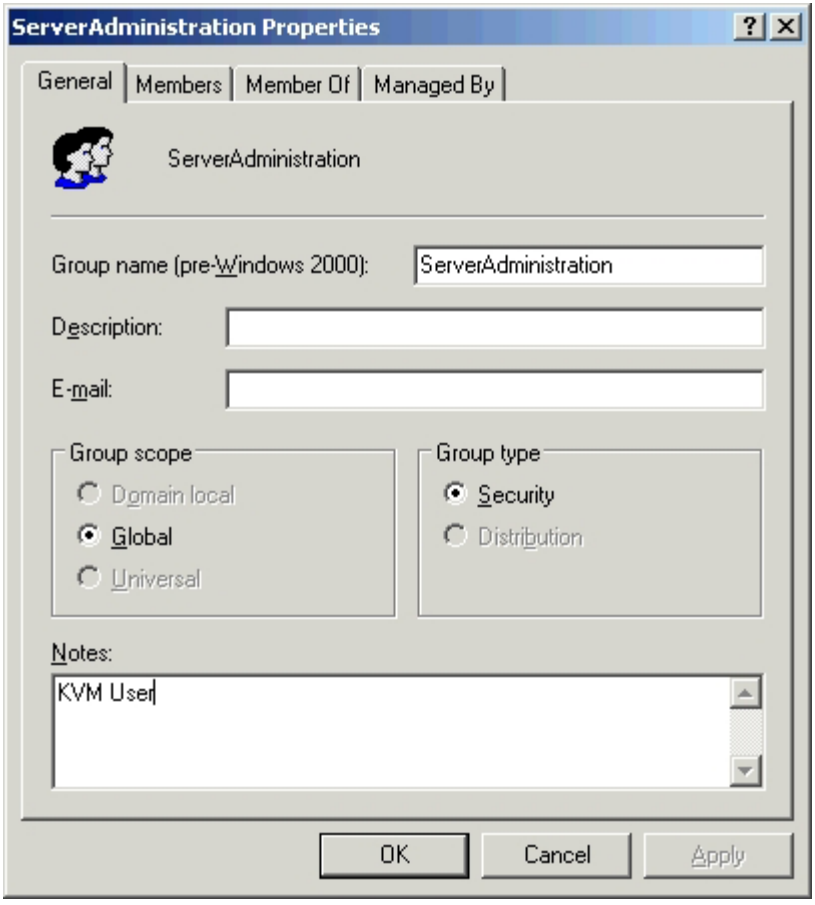

Figure 7-14: *KVM User* Attribute for *Group ServerAdministration*

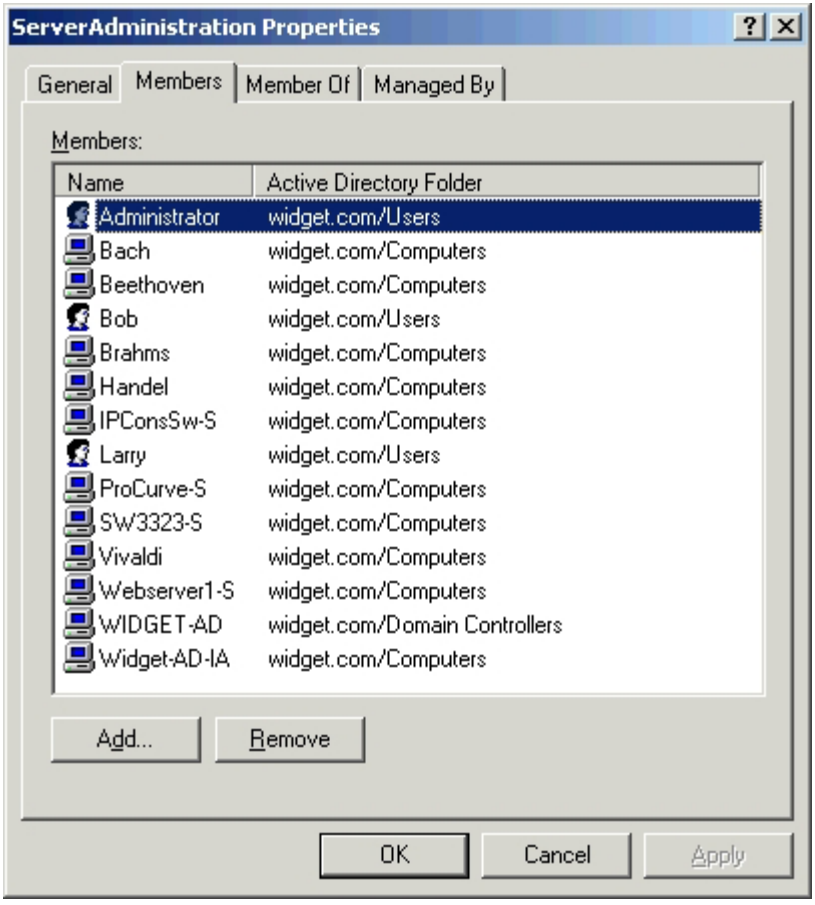

Figure 7-15: Members of Group *ServerAdministration*

Setting Up the Active Directory for Performing Group Attribute Mode Queries

Before you can use any of the querying modes for console switches or servers, first make changes to your Active Directory so that the selected querying mode can assign the correct authorization level for the user.

IMPORTANT: Before implementing LDAP functionality, refer to Appendix A for a better understanding of how LDAP works.

The following is an overview of how to set up group attribute mode queries. For more detailed information, refer to Appendix A.

To set up group attribute mode queries:

1. Name the Interface Adapters.
2. Install and launch the HP IP Console Viewer.
3. Discover or manually install a console switch.
4. Access the console switch.
5. Name the HP IP Console Switches.
6. Purchase the LDAP license key, and enable LDAP.
7. On the domain controller, add an OU group container.
8. Create a user, and assign a password.
9. Create groups for HP IP Console Switch admins and users.
10. Add the users and Interface Adapters to the appropriate groups.
11. From the HP IP Console Viewer application, log in to the HP IP Console Switch.
12. Test the LDAP communications from the HP IP Console Viewer application.

13. After the basic LDAP communication test succeeds, log in to the HP IP Console Switch from the HP IP Console Viewer application.

    NOTE: The console switch names and server names used for group attribute queries are stored in the console switches. The console switch name and server names specified in the SNMP and Servers categories of the Manage Console Switch must identically match the object names in the Active Directory. Each console switch name and server name might be composed of any combination of uppercase and lowercase letters (a–z, A–Z), digits (0–9), and hyphens (-). Spaces and per iods (.) are not allowed, and the name may not consist entirely of digits. These are Active Directory constraints. The factory default console switch name in earlier versions contains a space that must be removed by editing the system name in the SNMP category of the MP.

8

Accessing Remote Servers

You can access remote servers in the local database by selecting the All Servers folder in the group view or by clicking a particular remote server from the selected view. After you have selected a remote server, that remote server can be managed through the Video Session Viewer. The Video Session Viewer gives full keyboard, monitor, and mouse control to the user over a remote server.

You can also scan through a customized list of servers by enabling individual servers to display in the Thumbnail Viewer. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a screen image of the server. For more information, refer to the "Viewing Multiple Servers Using Scan Mode" section in Chapter 10.

To access a remote server:

1. Click the **Servers** icon in the main window.
2. Double-click the server name.

   -or-

   Select a server, then click the **Launch KVM Session** icon.

   -or-

   Right-click the server name, and select **Launch KVM Session.**

   -or-

   Select a server, and press the **Enter** key. The Video Session Viewer launches in a new window.

Searching for a Server in the Local Database

1. Click the **Servers** icon in the main window.
2. Insert your cursor in the Search text box, and enter the search information.
3. Click **Search.**
4. Review the results of your search.

   -or-

   Click **Clear Results** to display the entire list again.

Auto Searching for a Server in the List View

1. Click the **Servers** icon, then click any item in the List view.
2. Begin entering the first few characters of a server name. The highlight moves to the first device name beginning with those characters.

   To reset the search so you can find another device, pause for a few seconds, then enter the first few characters of the next server.

9

Managing Remote Servers

After you have connected to a server, the server desktop appears in a separate window called the Video Session Viewer. You see both the local and the server cursor. You might need to align these cursors if they do not move together or adjust the video if they seem to behave sporadically. For more information on aligning cursors, refer to the "Aligning the Cursors" section in this chapter.

From the Video Session Viewer, you can access all the normal functions of the server. You can also perform Viewer Session Viewer specific tasks, such as sending macro commands to the server.

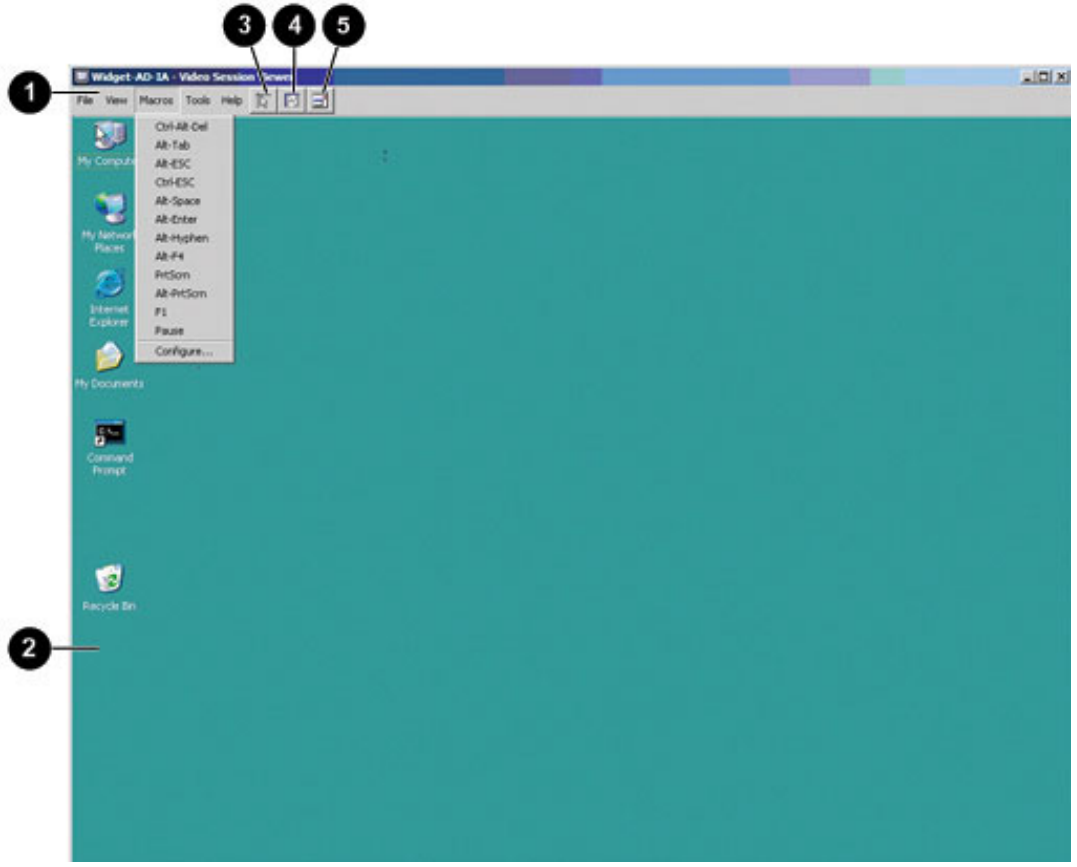

Figure 9-1: Video Session Viewer

Item	Description
1	Menu bar—Enables you to access features
2	Server desktop—Enables you to interact with the server through this window
3	Align Local Cursor icon—Enables you to reestablish proper tracking of the local cursor to the remote server cursor
4	Refresh Video icon—Enables you to regenerate the digitized video image of the server desktop
5	Full Screen mode icon—Enables you to expand the accessed server desktop to fill the entire screen

Expanding and Refreshing the Video Session Viewer

You can adjust your view using the three icons at the top of the Video Session Viewer. The first icon, Align Local Cursor, enables you to align the mouse cursors. The second icon, Refresh Video, enables you to refresh the video. The third icon, Full Screen mode, enables you to expand the Video Session Viewer. If you choose to expand the Video Session Viewer, the menu bar disappears, but you see a small floating palette with these three buttons, the macros dropdown list, and the server name.

Adjusting the Local Cursors

To adjust the local cursors, click the **Align Local Cursor** icon.

-or-

To adjust the local and remote cursors tracking, perform an **Automatic Video Adjust** from the Tools menu option.

Refreshing the Screen

To refresh the screen, click the **Refresh Video** icon.

-or-

From the Video Session Viewer menu, select **View>Refresh.** The digitized video image is completely regenerated.

Expanding to Full Screen Mode

To expand to full screen mode, click the **Full Screen** icon.

-or-

From the Video Session Viewer menu, select **View>Full Screen.** The desktop window disappears, and only the accessed server desktop is visible. The screen resizes up to 1024 x 768. If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar appears.

To exit full screen mode, click the **Full Screen** icon on the floating toolbar.

Adjusting the Video Session Viewer

You can adjust both the resolution and quality of the Video Session Viewer. You can also expand your session to fit the entire screen or refresh the view at any time.

Adjusting the Video Session Viewer Size

The Video Session Viewer enables you to set up automatic scaling or manual scaling for the viewer window. When Auto Scale is selected, the desktop stays the same size and the Video Session Viewer scales to fit the desktop. When manual scale is selected, a list containing a selection of supported Video session Viewer sizes appears.

To adjust the size of the Video Session Viewer size:

Select **View>Auto Scale** to scale the Video Session Viewer automatically.

Adjusting the Video Quality

The Video Session Viewer offers both automatic and manual video adjustment capability. In most instances, the Automatic Video Adjustment optimizes the video for the best possible view.

The Performance Monitor provides feedback while adjusting the settings. Adjust the settings until the Performance Monitor displays no values.

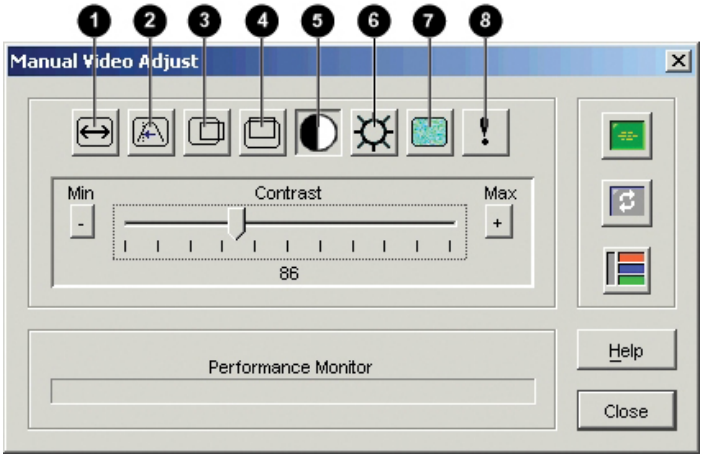

Figure 9-2: Manual Video Adjust dialog box

Item	Description
1	Image Capture Width—Adjusts the screen image width
2	Pixel Sampling Fine Adjust—Adjusts the screen image pixel sharpness
3	Image Capture Horizontal Position—Adjusts the screen image position left or right
4	Image Capture Vertical Position—Adjusts the screen image vertical position up or down
5	Contrast—Increases or decreases screen image lightness or darkness
6	Brightness—Increases or decreases screen image intensity
7	Noise Threshold—Adjusts the number of pixels in a block for which a change must be detected for the video data to be sent to the client
8	Priority Threshold—Adjusts the level of changes within a video block to determine what would be sufficient to cause a video block to be marked as high priority

To adjust the video quality of the Video Session Viewer window:

1. Select **Tools>Manual Video Adjust.** The Manual Video Adjust dialog box appears.
2. Click the icon to be adjusted, and move the slider bar or click the **Min -** or **Max +** buttons. The adjustments are displayed immediately.
3. Click **Close** to exit.

Adjusting the Mouse Settings

IMPORTANT: For Windows servers, mouse scaling should not be used. Adjust the mouse settings for the server using the following instructions in this section. If after following these instructions the mouse pointers track properly but are not perfectly aligned, readjust the video by selecting **Tools**>**Automatic Video Adjust.**

The Video Session Viewer enables you to select among five different mouse cursor options, set up mouse scaling, and resynchronize your mouse, should it no longer track properly. Mouse settings are target device-specific and can be set differently for each device.

To adjust the mouse settings:

1. Select **Tools>Session Options.** The Session Options dialog box appears.

   NOTE: The Session Options dialog box only controls the settings for the selected server. The file name of the selected server appears after Session Options in the Session Options dialog box title bar.

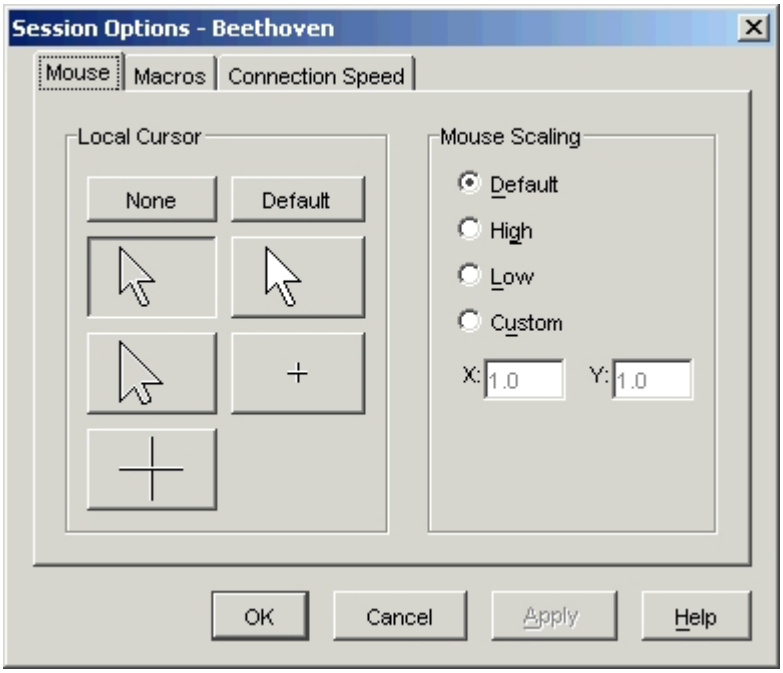

Figure 9-3: Session Options dialog box

2. Select the **Mouse** tab, and click the desired cursor icon to be adjusted.
3. Click **Apply** to view the changes, then click **OK** to exit.

Mouse Tuning

To have the mouse pointers synchronized, you must change the mouse settings on the target server you will be controlling remotely.

NOTE: HP recommends that all Windows systems attached to the console switch use the default Windows PS/2 mouse driver.

Windows Operating Systems

To synchronize the mouse pointers for Windows operating systems (using the default drivers):

1. From the desktop, select **Start>Settings>Control Panel,** and double-click the **Mouse** icon.
2. Select the **Motion** tab.
3. For Windows 2000, set the Speed setting to **50%** (default) and the Acceleration setting to **None.**

   -or-

   For Windows Server 2003, set the set the Speed setting to **50%** (default) and deselect the Enhance Pointer Precision checkbox.

Linux Operating Systems

NOTE: The following Linux example uses Red Hat 3.0. For more information, refer to your Linux operating systems HELP, or documentation.

To synchronize the mouse pointers for Linux operating systems (GNOME):

1. Click **main** menu.
2. From the main menu task list, select **Programs>Settings>Peripherals.**
3. From the Peripherals task list, select **Mouse.** The Mouse Configuration window appears. In this window, you can set the mouse to be either right-handed or left-handed and adjust the mouse motion by changing the threshold and adjusting the acceleration to the fourth position from the far left.

To synchronize the mouse pointers for Linux operating systems (KDE):

1. Go to the main menu, and select **K Menu>KDE Control Center>Input Devices>Mouse.**
2. Set the acceleration to **1X.**
3. Apply the settings, and then click **OK.**

Aligning the Cursors

If the cursors no longer respond properly, you can align them to reestablish proper tracking. Alignment causes the local cursor to align with the cursor on the remote server.

CAUTION: If the server does not support the ability to disconnect and reconnect the cursors (almost all new PCs do), then the cursor becomes disabled and the server must be rebooted.

To align the cursor for most operating systems, click **Align Local Cursor** in the menu bar.

Viewing Multiple Servers Using Scan Mode

The Video Session Viewer enables you to simultaneously view multiple servers through the Thumbnail Viewer of Scan mode. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a server's screen image. The server name and status indicator appears below each thumbnail. The default thumbnail size is based on the number of servers in the scan list.

Scanning Your Servers

Through the Thumbnail Viewer, you can set up a scan sequence of up to 16 servers to monitor your servers. Scan mode moves from one thumbnail image to the next, logging in to a server and displaying an updated server image for a user-specified length of time (View Time Per Service), before logging out of that server and moving on to the next thumbnail image. You can also specify a scan delay between thumbnails (Time Between Servers). During the delay, you see the last thumbnail image for all servers in the scan sequence, though you will not be logged in to any servers.

When you first launch the Thumbnail Viewer, each frame is filled with a white background until a server image appears. An indicator light at the bottom of each frame displays the status of the server. A green LED indicates that a server is currently being scanned. A red X LED indicates that the last scan of the server was not successful. The scan might have failed because of a credential or path failure (the server path on the HP IP Console Switch was not available). The tool tip for the LED indicates the reason for failure.

Scan mode is a lower priority than an active connection. If you have an interactive session with a server, that server is omitted in the scan sequence and the scan proceeds to the next server. No login error messages display. After the interactive session is closed, the server is included in the scan sequence again. If another user has an active connection to a server, you see that thumbnail in your scan list.

Accessing Scan Mode

1. From the HP IP Console Viewer, select the **Server, Sites,** and **Folders** tabs.
2. Select two or more servers by clicking the servers while pressing the **Shift** key or the **Control** key. The Scan Mode button appears.

3. Click **Scan Mode.** The Scan Mode window appears.

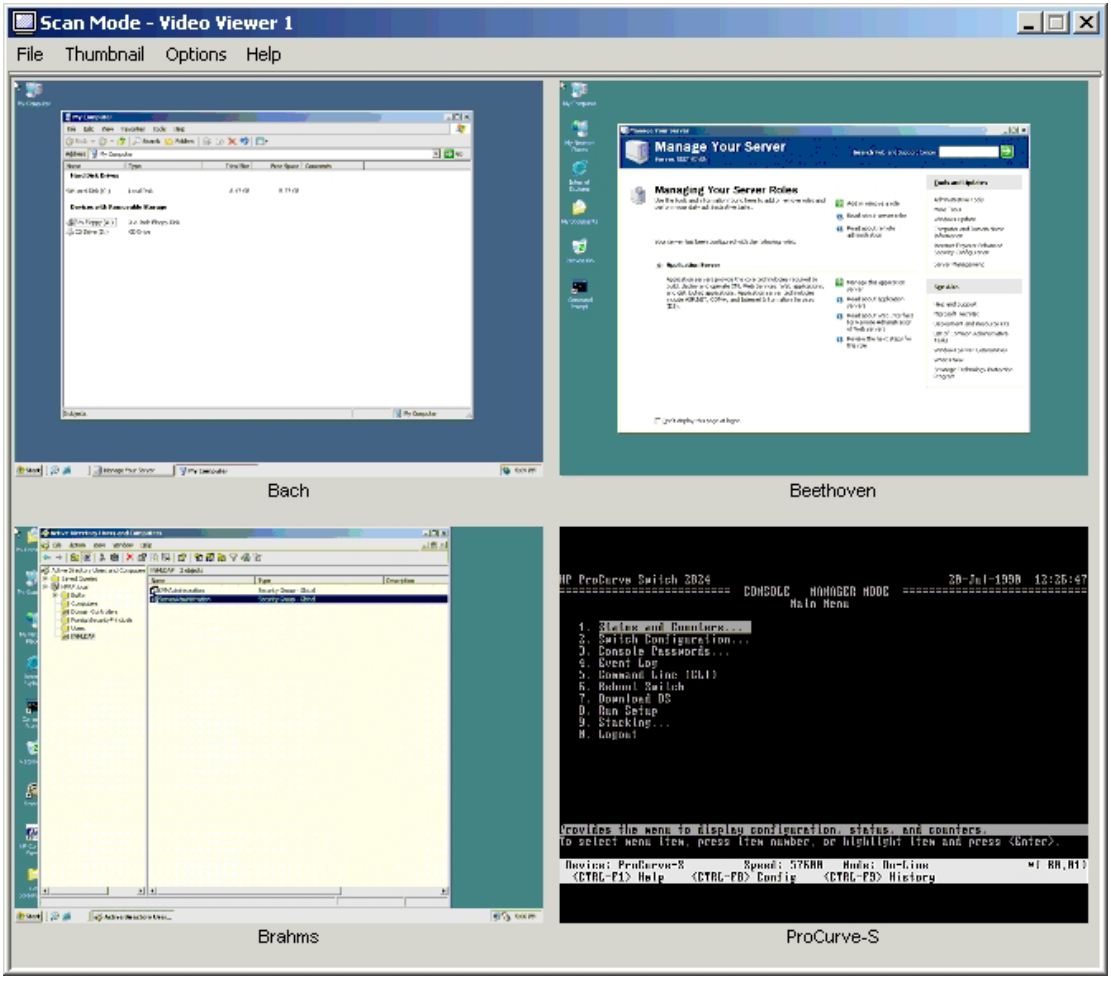

Figure 9-4: Video Session Viewer thumbnail view

Setting Scan Preferences

1. From the thumbnail view, select **Options>Preferences.** The Scan Mode Preference dialog box appears.
2. Enter the time each thumbnail is active during the scan (5 to 60 seconds) in the View Time Per Server field.
3. Enter the length of time the scan stops between each server (1 to 60 seconds) in the Time Between Servers field.

4. Click **OK** or **Cancel** to exit.

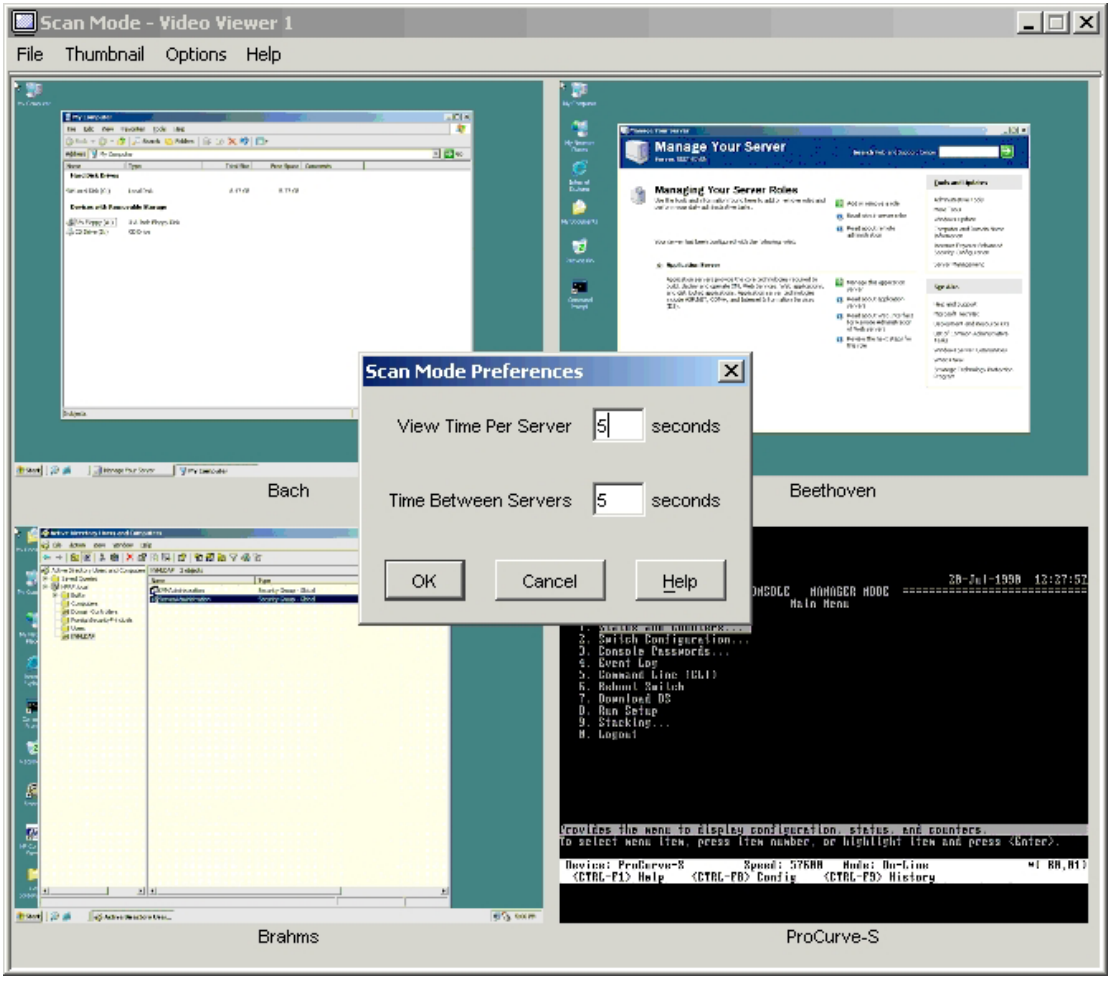

Figure 9-5: Scan Mode Preferences

Navigating the Thumbnail View

When you highlight an individual thumbnail frame and select the Thumbnail menu, you can launch an interactive session to that server, add that server to the scan sequence, or set the login credentials for that server.

The Options menu enables you to access scanning preferences, pause the scan, and set the thumbnail size for all servers.

Launching a Server Video Session from a Thumbnail View

Select a server thumbnail. From the Thumbnail Viewer, select **Thumbnail>[*servername*]>View Interactive Session.**

-or-

Right-click a server thumbnail, and select **View Interactive Session.** The video for that server launches in an interactive Video Session Viewer window.

-or-

Double-click a server thumbnail.

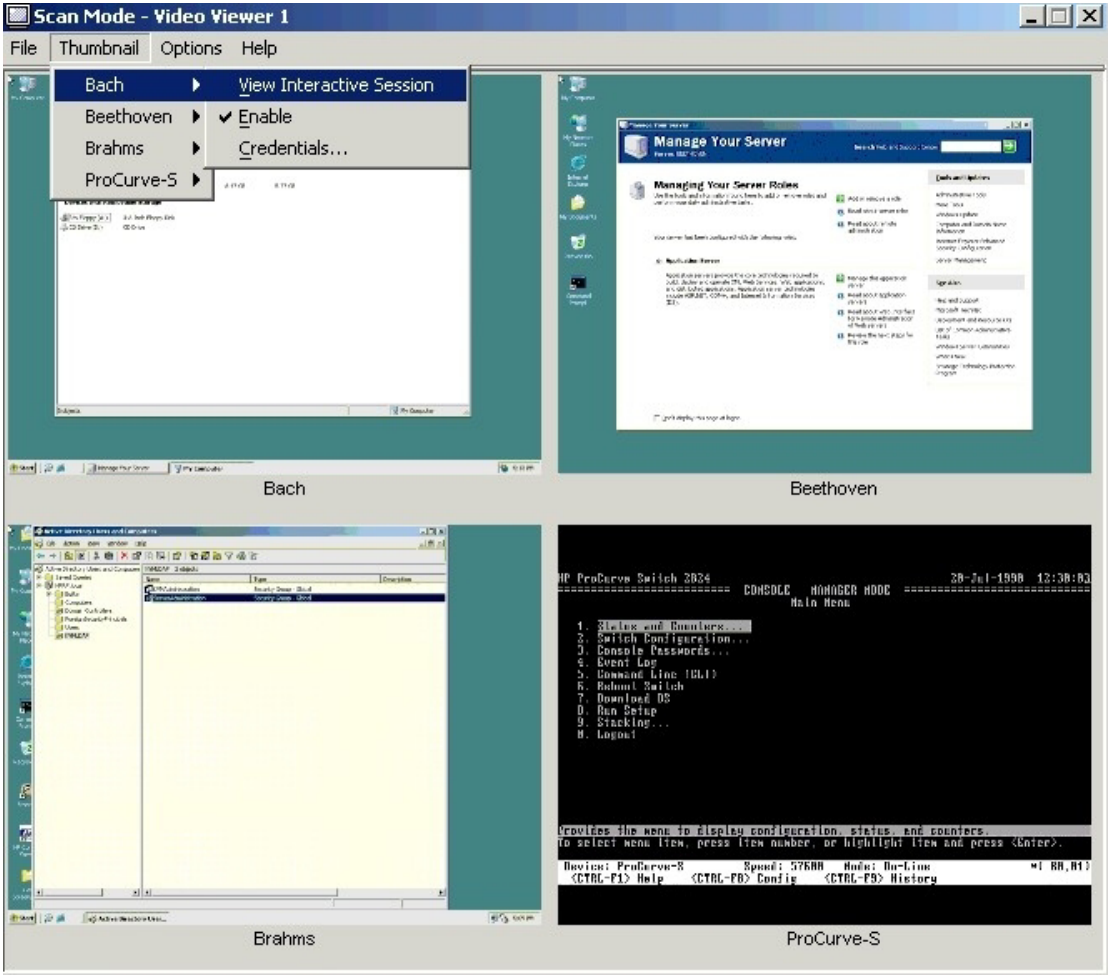

Figure 9-6: Scan Mode thumbnail view

Adding an Individual Server to the Scan Sequence

1. From the Scan Mode thumbnail view, right-click a server thumbnail.
2. Select **Thumbnail,** and then select **Enable.**

   That scan includes the server thumbnail in the scan sequence.

NOTE: If a user is accessing a server, the Enable Scan menu is disabled for that server thumbnail.

Setting Server Credentials

1. Select a server thumbnail.

   From the Thumbnail View, select **Thumbnail>[*servername*]>Credentials.**

   -or-

   Right-click a server thumbnail, and select **Credentials.** The login dialog box appears.
2. Enter a user name and password for the selected server. Press the **Enter** key.

Pausing or Restarting a Scan Sequence

From the Thumbnail Viewer, select **Options>Pause Scan.** The scan sequence pauses at the current thumbnail, if the Thumbnail Viewer has a scan in progress, or restarts the scan if currently paused.

Changing the Thumbnail Sizes

From the thumbnail viewer, select **Options>Thumbnail Size.** Select the desired thumbnail size from the cascade dropdown list.

Using Macros

The Macros menu in the Video Session Viewer provides you with an easy way to send multiple keystrokes to a server or send keystrokes that you cannot generate without affecting your local system, such as Ctrl-Alt-Delete.

The Video Session Viewer provides a list of default keystroke selections. However, using the Configure option at the bottom of the Macros dropdown list can set up custom macros.

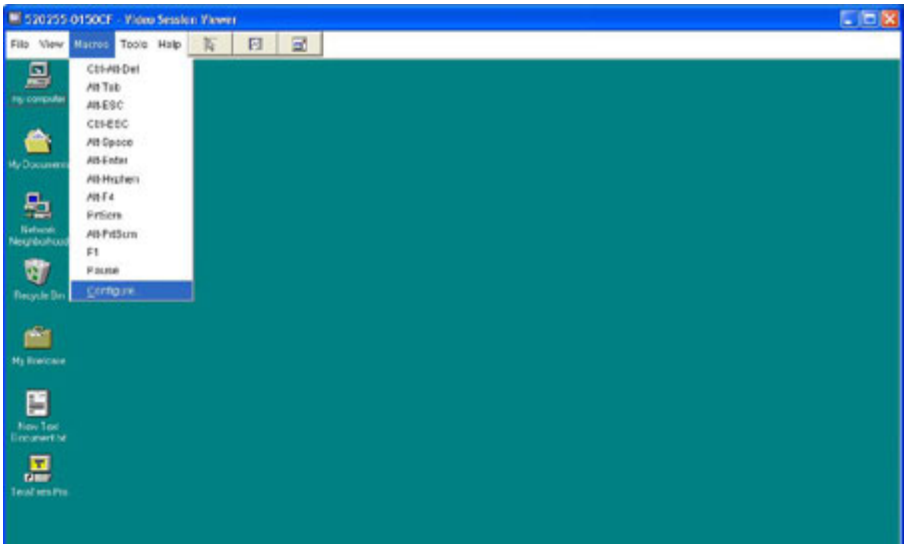

Figure 9-7: Macros menu

To send keystrokes to the server, click **Macros,** and then select the macros to send.

Sending Keystrokes to a Device

Select the **Macros** menu in the Video Session Viewer, and select the macro to send to the server. If the keystroke you want is not in the list, select **Configure** to access the Macros dialog box. Here you can create, modify, delete, and group macros.

Macro group settings are specific to each target device and, therefore, can be set differently for each server. These settings are placed in to the local client database and applied each time you launch a session to a specific device.

Changing Default Macro Groups

1. From the Manage Console Switch, select **Tools>Session Options.** The Session Options dialog box appears.
2. Select the **Macros** tab.

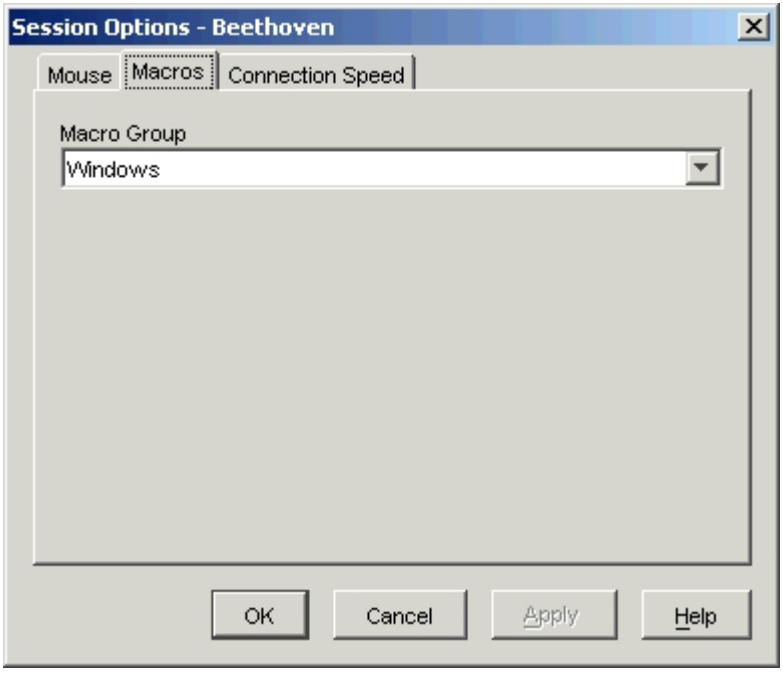

Figure 9-8: Session Options dialog box

3. Select the macro group from the **Macro Group** dropdown list.
4. Click **OK,** or click **Cancel** to exit.

Creating New Macros

You can create custom macro keystrokes, as well as edit and delete existing macros through the Macros dialog box.

To create a new macro:

1. From the Manage Console Switch, select **Macros>Configure.** The Macros dialog box appears.
2. Click **Create.** The Create Macro dialog box appears.

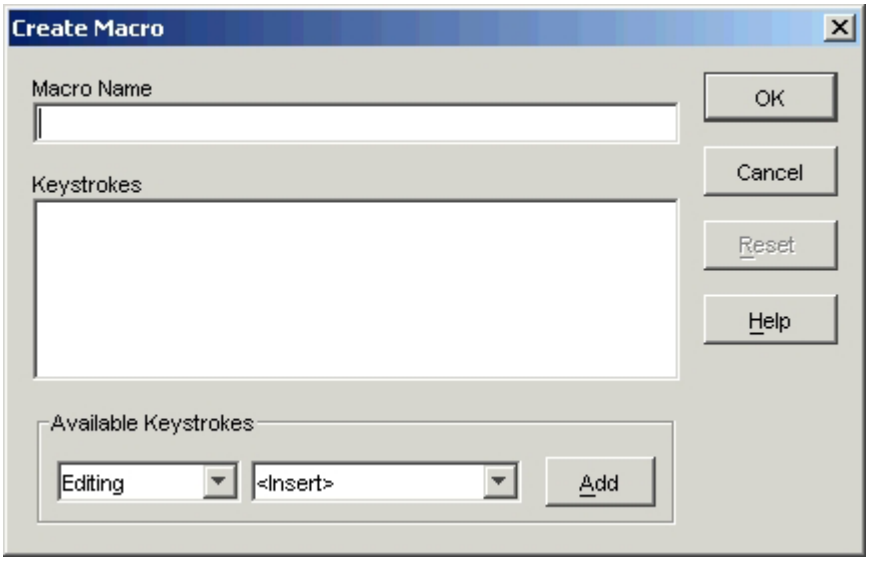

Figure 9-9: Create Macro dialog box

3. Enter the name of the macro in the Macro Name field.
4. Select the desired category and keystrokes from the list of Available Keystrokes and click **Add.**

   -or-

   Enter the keystrokes in the Keystrokes field.

   To enter a keystroke, such as Enter, Home, or Insert, surround each individual keystroke with a less than (<) and a greater than (>) symbol.

   -or-

   To enter a letter or number, enter the letter or number without any additional symbols.

   -or-

   For auxiliary keystroke, such as Control, Shift, or Alt, where a press, hold, and release are required to complete a command, enter the initial press keystroke (such as <Ctrl-Press>), then the keystroke, letter, or number of the command, followed by the closing release (such as <Ctrl-Release>).
5. Click **OK** to accept the macro and return to the Macros dialog box.

   -or-

   Click **Reset** to erase all the keystrokes entered in the Keystrokes field.

   -or-

   Click **Cancel** to exit.
6. Click **Close** to exit the Macros dialog box.

Grouping Macros

The Macro Groups dialog box enables you to group macros into logical groups. Macro groups for Windows are already predefined, but the groups can be altered or you can create an entirely new group. You can also rename and delete groups that have been previously created.

To create a macro group:

1. Select **Macros>Configure.** The Macros dialog box appears.
2. Click **Group.** The Macro Groups dialog box appears.

3. Click **Create.** A dialog box appears prompting you to name the macro groups.

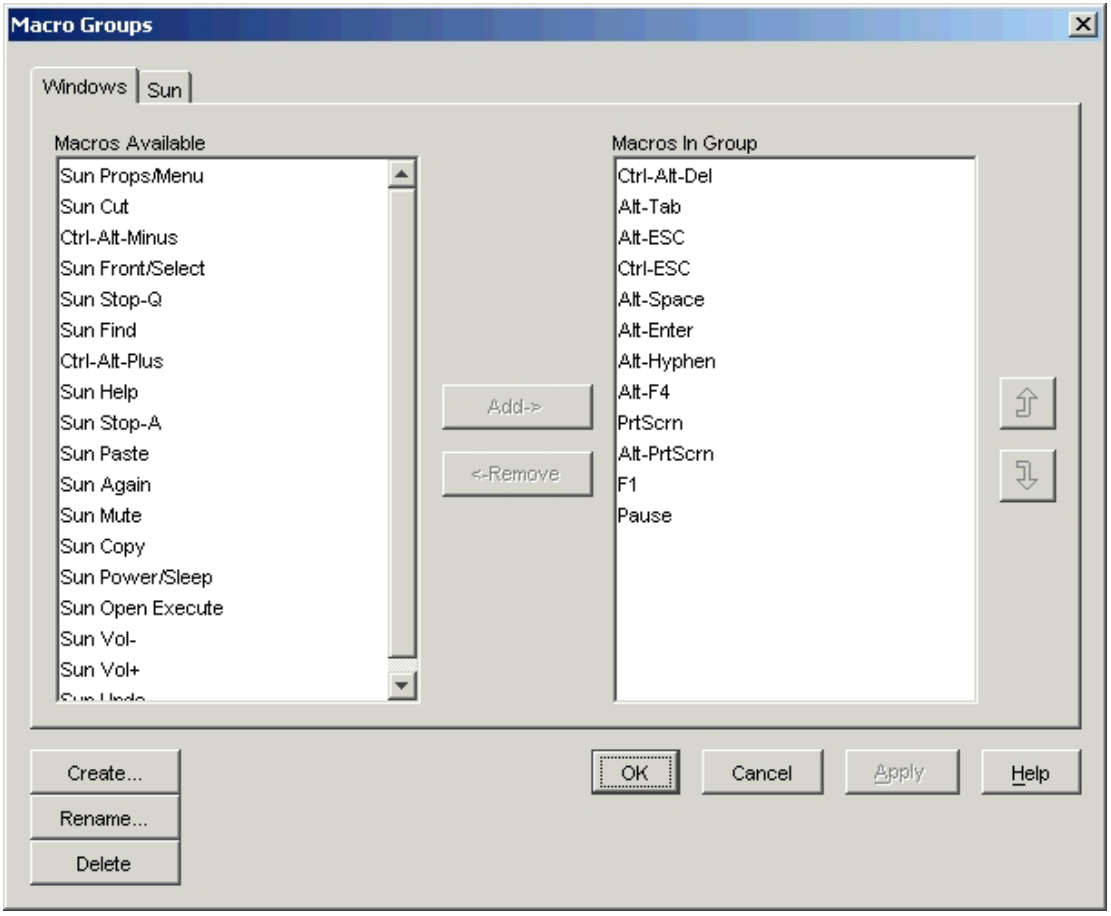

Figure 9-10: Macro Groups dialog box

4. Enter the desired name, and click **OK** to save the name and return to the Macro Groups dialog box. A tab with the new name appears.

Adding Macros to an Existing Group

1. Select **Macros>Configure.** The Macros dialog box appears.
2. Click **Group.** The Macro Groups dialog box appears.
3. Select the actual macro to be added from the Macros Available list on the left side of the dialog box.
4. Click **Add.** The macro appears in the Macros in Group list. Click the **Move Up** and **Move Down** buttons to move the macro up or down.
5. Repeat steps 3 and 4 until all the macros are displayed in the Macros in Group list.
6. Click **Apply,** then click **OK** to accept the macro group and return to the Macros dialog box.

   -or-

   Click **Cancel** to exit.

Renaming Macro Groups

The Rename button enables you to rename an existing macro group. Click **Rename** to rename an existing macro group.

Connection Speed

The Connection speed tab of the Session options dialog can be used to optimize the video connection. The value selected in this tab is used to throttle the video stream based on the available bandwidth, which allows the system to optimize its operation.

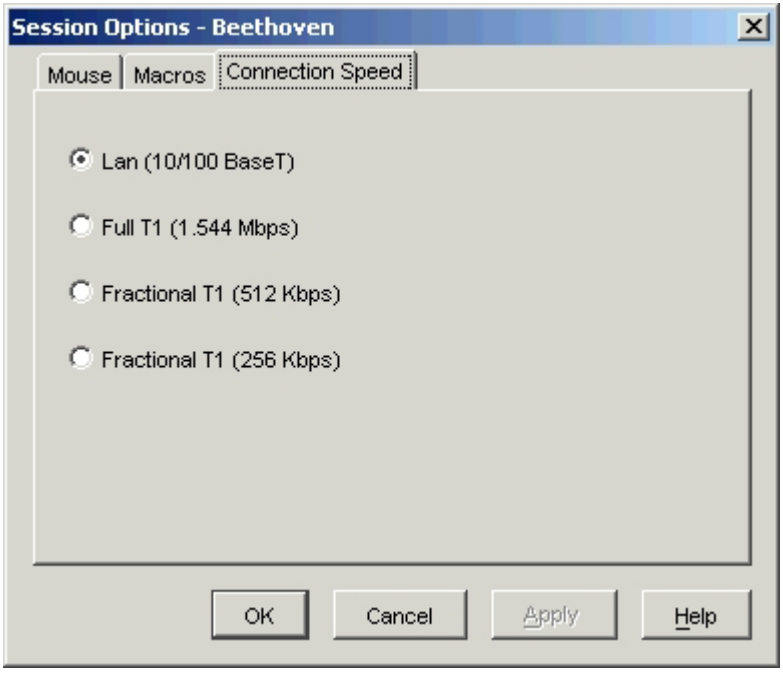

Figure 9-11: Connection speed

Preemption Mode

Preemption provides a means for users with sufficient access level to take control of a server from another (remote or local) user with lesser or equal access level. Depending on the access level of the user issuing the preemption request and that of the user being preempted, the preemption request can be rejected.

Table 9-1: Preemption Scenarios

User Level	Preempted By	Can the Preemption be Rejected?
Local User	Console Switch Admin	Yes
Console Switch Admin	Local User	Yes
Console Switch Admin	Console Switch Admin	Yes
Remote User	Local User	No
Remote User	Console Switch Admin	No

NOTE: The Override Admin account is treated as a Console Switch Admin in the above preemption scenarios.

Selecting Server Properties

The Properties dialog box for servers contains several tabs:

- **General**—Enables you to change the server name, server type, and server icon and to assign the server site, location, or folder
- **Network**—Enables you to establish a browser URL for that server
- **Information**—Enables you to enter information about the server, including a server description, contact information, and any comments you might want to add
- **Connections**—Enables you to display connection options for that server

To change server properties:

1. Select an individual server from the selected view.
2. Select **View>Properties** from the menu bar. The General tab appears.

   -or-

   Click **Properties.** The General tab appears.

   -or-

   Highlight and right-click the server, then select **Properties.** The General tab appears.

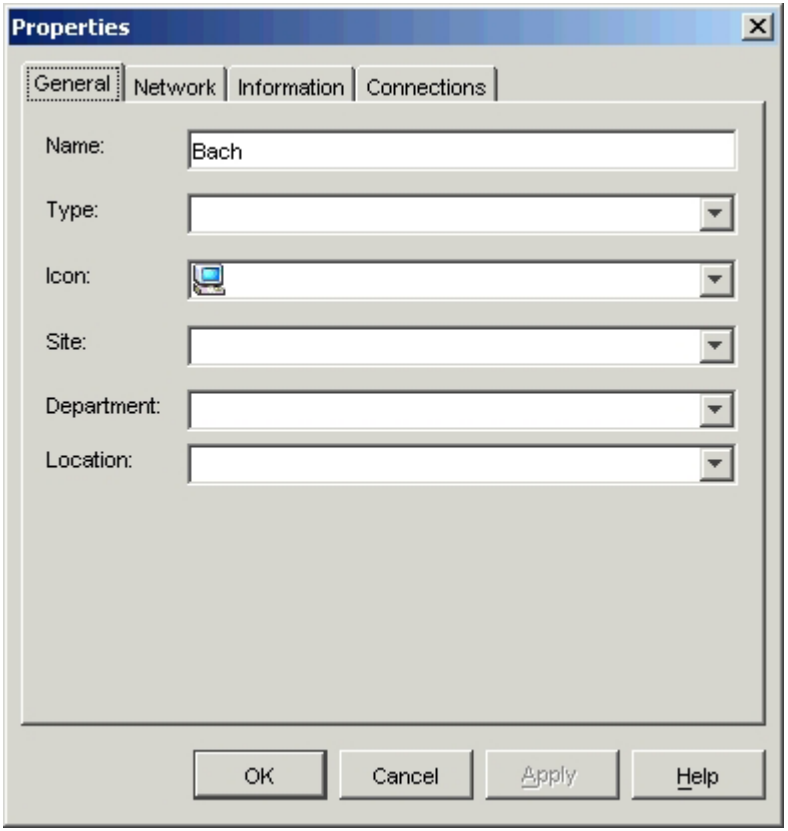

Figure 9-12: General tab

3. (Optional) Select the server type (user definable). If the selection is not in the dropdown list, enter the name of the new type.
4. (Optional) Select the icon to display for the server.
5. (Optional) Select the site, department, and location. If the selection is not in the dropdown list, enter the name of the new assignment.
6. (Optional) Select the **Network** tab, and enter a URL into the Browser URL field. The field is optional and can be left blank. If the field contains a value, then the Browse button appears in the Task window, allowing the browser to that specified URL to launch.

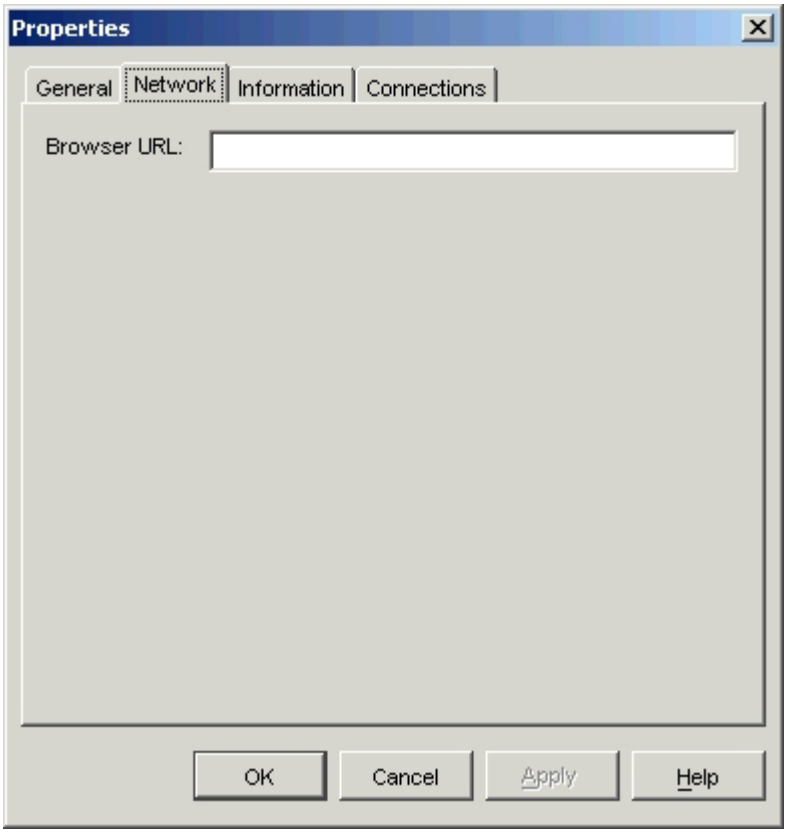

Figure 9-13: Network tab

7. (Optional) Select the **Information** tab, and enter the information.

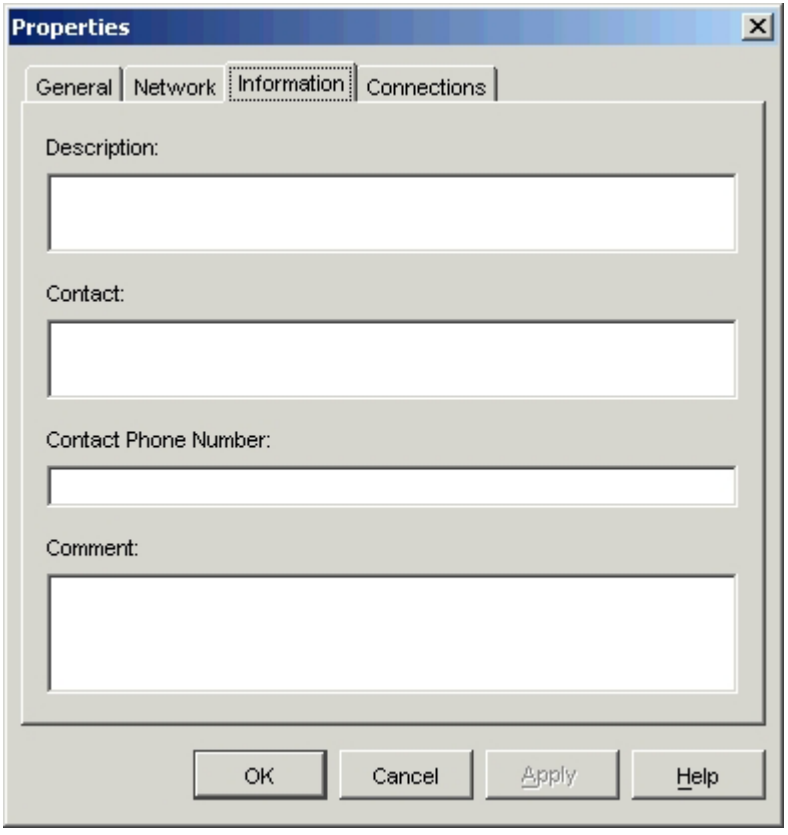

Figure 9-14: Information tab

8. Select the **Connections** tab to view the connection path.

   If a server is attached to a cascade console switch, then the connection sequence is as follows: connection type (video), console switch name with IP address in parentheses, Interface Adapter port number, Interface Adapter ID, cascade console switch name, channel server that the cascade console switch is connected to, and the server name.

If a server is connected directly into a console switch or an expansion module, then the connection sequence is as follows: console switch name with IP address in parentheses, Interface Adapter port number, Interface Adapter ID, and the server name.

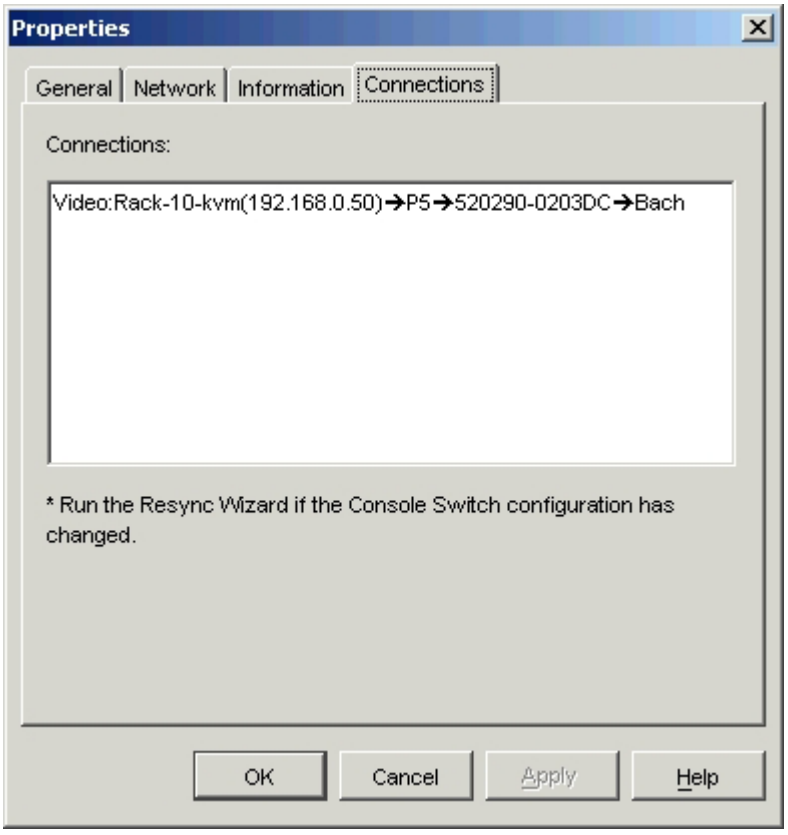

Figure 9-15: Connections tab

9. Click **Apply,** then click **OK** to save the new settings.

   -or-

   Click **Cancel** to exit.

10

Organizing the System

The Sites and Folder view tabs enable you to organize and manage your console switches and servers by custom groups. Site organization is based on where your servers are located and refers to the column headings Site and Department, which can be customized to suit your needs.

Creating Custom Field Labels

The custom field label enables you to change the Site, Department, and Location names of the column headings that display in the group and selected views This functionality enables you to group and sort console switches and servers in ways that are meaningful to you. The Department field is a subset of Site. If you customize these field names, you should keep this hierarchy in mind.

Setting Up Custom Field Labels

1. From the Main menu, select **Tools>Options.** The Options dialog box appears.

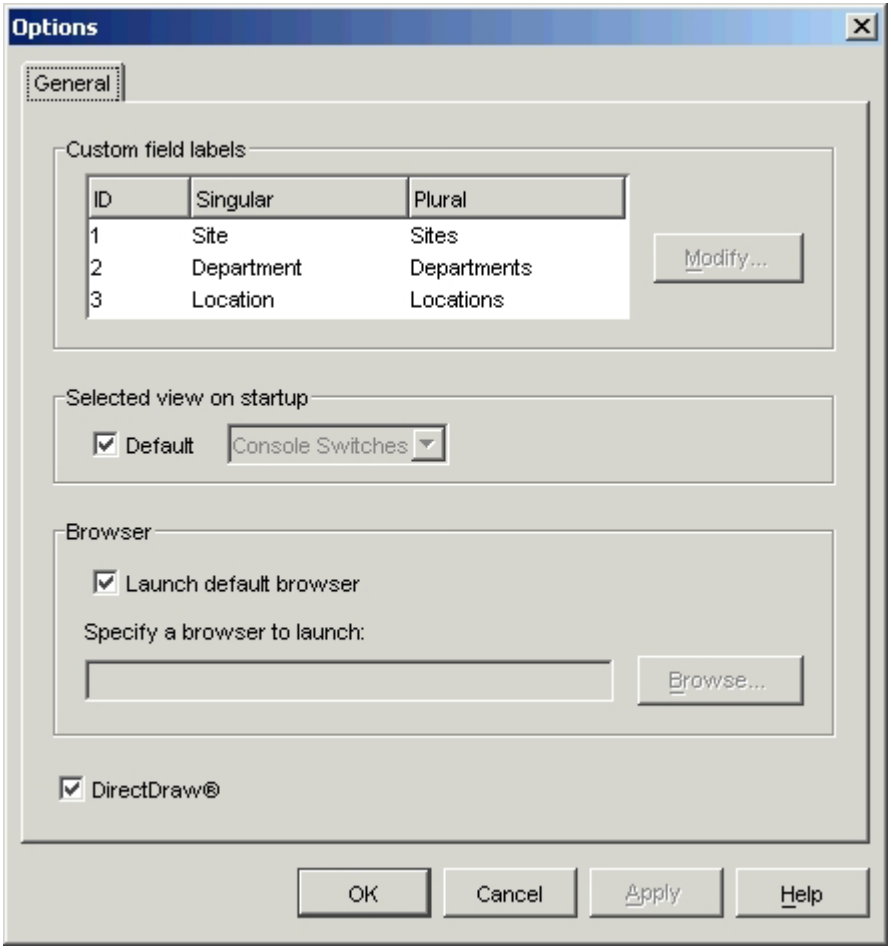

Figure 10-1: Options dialog box

2. Select a custom field label.
3. Click **Modify.** The Modify Custom Field dialog box appears

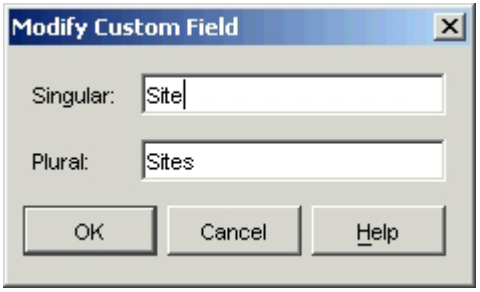

Figure 10-2: Modify Custom Field dialog box

4. Enter the singular and plural versions of the field label. The length can be from one to 32 characters. A blank value is not allowed. Spaces are allowed in the middle, but leading and trailing spaces are not allowed. The label can consist of any combination of characters that can be entered from the keyboard.
5. Click **Apply,** then click **OK.**

   -or-

   Click **Cancel** to exit.

Creating New Sites, Departments, or Locations

1. Select **View>Properties.**

   -or-

   Select the device, and click **Properties.** The Properties dialog box appears.

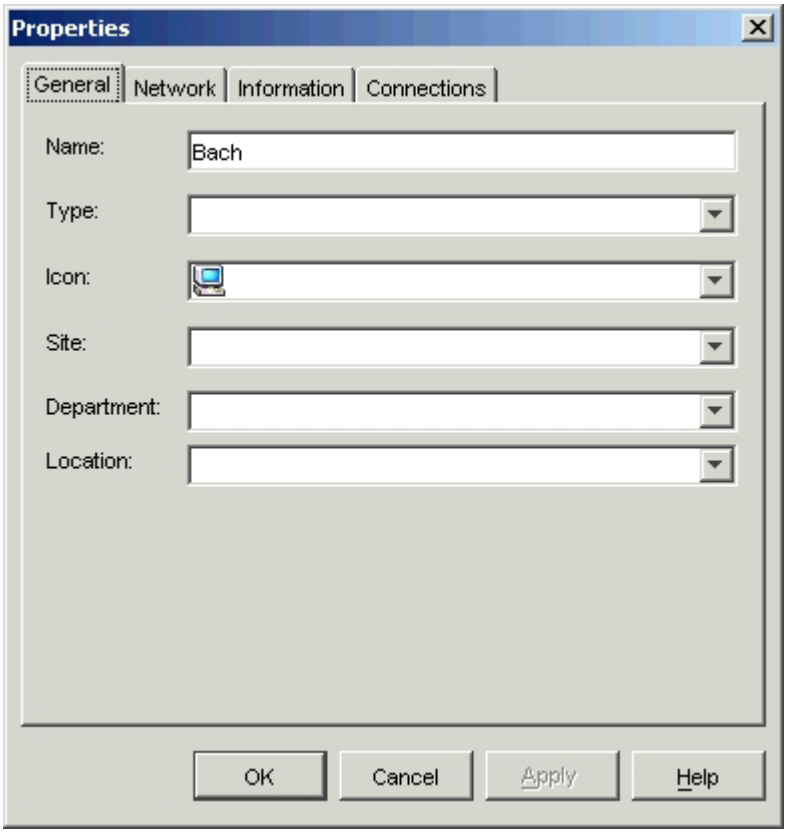

Figure 10-3: General tab

2. Select the **General** tab, and select the site, department, or location from the dropdown list.

   NOTE: The dropdown lists are empty until you enter more than one name for the selected category.

3. Enter a name one to 32 characters long. Names are not case-sensitive and can consist of any combination of characters entered from the keyboard. Spaces are allowed in the middle, but leading and trailing spaces are not allowed. Duplicate names are not allowed.
4. Click **Apply,** then click **OK.** The new site, department, or location is displayed in the group view.

Creating New Folders

1. Select **Folders** in the icon view.
2. Click the **Folders** directory, and select **File>New>Folder** from the task bar. The New Custom Folder dialog box appears.
3. Enter a name one to 32 characters long. Names are not case-sensitive and can consist of any combination of characters entered from the keyboard. Spaces are allowed in the middle, but leading and trailing spaces are not allowed. Duplicate names are not allowed at the same level but are allowed across different levels.
4. Click **Apply,** then click **OK.** The new folder is displayed in the group view.

Assigning Devices to Sites, Departments, Locations, or Folders

You can assign a console switch or server to a site, department, location, or folder. This menu item is only enabled when a single console switch or server is selected in the selected view. These custom targets are defined in the General tab of the Properties dialog box.

To assign a device to a site, department, location, or folder:

1. Select the device in the selected view.
2. Select **Edit>Assign To** in the menu bar, or click **Assign To** in the Task window. The Assign To dialog box appears.

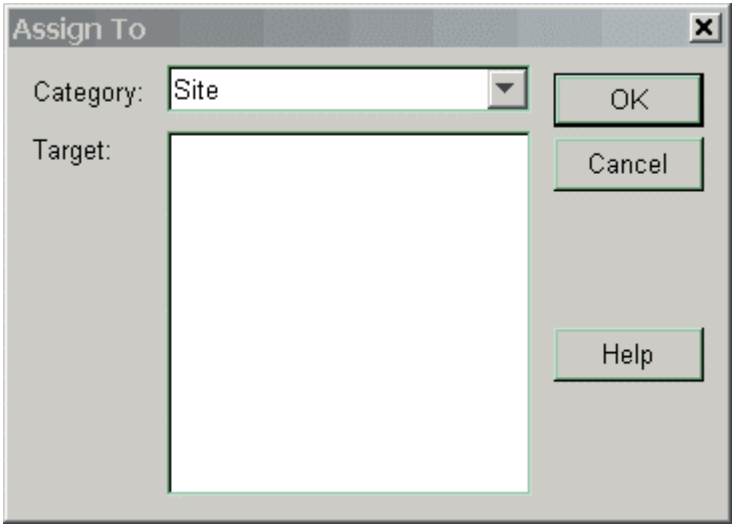

Figure 10-4: Assign To dialog box

3. Select the category **(Site, Department, Location,** or **Folder)** from the dropdown list.
4. Select the target from the list of available targets that the console switch can be assigned to within the selected category. This list is empty if no site, department, location, or folder has been defined in the local database.

5. Click **OK** to save the assignment.

   -or-

   Click **Cancel** to exit.

To drag and drop a device into a site, department, location, or folder:

1. From the Main menu, click and hold the desired row in the selected view.
2. Drag the item to the desired directory in the group view, and then release the mouse button.

NOTE: A device cannot be moved to All Departments, All Console Switches, All Servers, or root Sites directory. Devices can be moved only one at a time.

Deleting and Renaming a Device

The delete function is context-sensitive, based on what is currently selected in the group and selected views. When a device in the selected view is selected and deleted, the device is removed from the local database. When an item is selected and deleted in the tree view of the group view, you can delete server types, sites, departments, location, and folders. However, none of these actions results in console switches being deleted from the local database. The HP IP Console Viewer also provides the ability to rename items in the database, including individual devices, sites, departments, locations, and folders.

NOTE: If you have an OSD on an analog port and you delete or rename a server through the HP IP Console Viewer, the OSD server list becomes out of date. Servers should be deleted or renamed from the OSD.

Deleting a Device, Site, Department, Location, or Folder

1. Select the device, site, department, location, or folder to be deleted from the group view.
2. Select **Edit>Delete.** A dialog box appears, confirming the number of devices affected by this deletion.

   -or-

   Press the **Delete** key.
3. Click **Yes.** Additional message prompts might appear, depending on the configuration.

Renaming a Device, Site, Department, Location, or Folder

1. Select the device, site, department, location, or folder.
2. Select **Edit>Rename.** The Rename dialog box appears.
3. Enter a name one to 32 characters long. Names are not case-sensitive and can consist of any combination of characters entered from the keyboard. Spaces are allowed in the middle, but leading and trailing spaces are not allowed. Duplicate names are not allowed, with the exception of departmental names, which can be duplicated across different sites, and folder names, which can be duplicated across different levels.
4. Click **Apply,** then click **OK.**

   -or-

   Click **Cancel** to exit.

Customizing the Main Window

The main window can be resized. Each time the HP IP Console Viewer is displayed, the window appears in the default size and location. The default size and location can be changed while the application is running, but the information is not saved.

A split-pane divider runs from the top to the bottom and separates the group view and the selected view. The divider can be moved left and right to change the viewing area of the group view and selected view. Each time the HP IP Console Viewer is displayed, the divider appears in the default location.

Modifying the Selected View on Startup

You can modify the startup window, or main window, when the HP IP Console Viewer is displayed. When the default option is selected, the main window determines which view to display, based on the console switches defined in the local database. When the default option is deselected, the main window displays the view selected in the dropdown list. The dropdown list is enabled only when the default checkbox is deselected.

To modify the selected view on startup:

1. Click **Tools>Options.** The Options dialog box appears.
2. Select the default checkbox, and click **OK** to exit.

   -or-

   Leave the default checkbox deselected, and proceed to step 3.
3. Select either **Console Switches, Servers, Sites,** or **Folders** from the dropdown list.
4. Click **Apply,** then click **OK** to save the changes.

   -or-

   Click **Cancel** to exit.

Changing the Default Browser

You can specify which browser is displayed when a server URL in a browser window is viewed. You can select a specific browser or use the default browser.

To change the default browser:

1. Select **Tools>Options.** The Options dialog box appears.
2. Deselect the **Launch Default Browser** checkbox. The Browser button is enabled.
3. Click the **Browse** button, and navigate to the browser.
4. Click **Apply,** then click **OK** to save the changes.

   -or-

   Click **Cancel** to exit.

Using Direct Draw

Direct Draw is a standard that enables direct manipulation of video display memory, hardware video data transfers, hardware overlays, and page flipping without the intervention of the Graphics Device Interface (GDI). This direct path results in smoother animation and display-intensive software that runs faster and avoids screen flicker. By default, Java™ uses Direct Draw to enhance performance of the video.

Managing Local Databases

Each server running HP IP Console Viewer contains a local database that records all of the information that is entered about the devices. If multiple servers or workstations access a device, you can configure them and save a copy of the database and load it onto other servers and workstations to avoid reconfiguring each one. You can also export the database for use in another application.

Saving Local Databases

The HP IP Console Viewer enables you to save a copy of the local database. The saved database can then be loaded back to the same computers on which it was created, or it can be loaded on another HP IP Console Viewer client station. The saved database is compressed into a single .ZIP file.

While the database is being saved, no other activity is allowed. All other windows, including Video Session Viewer and Manage Console Switch windows, must be closed. If other windows are open, a message appears, prompting you to either continue, which closes all open windows, or quit, which cancels the database save process.

To save a local database:

1. Select **File>Database>Save.** The Database Save dialog box appears.

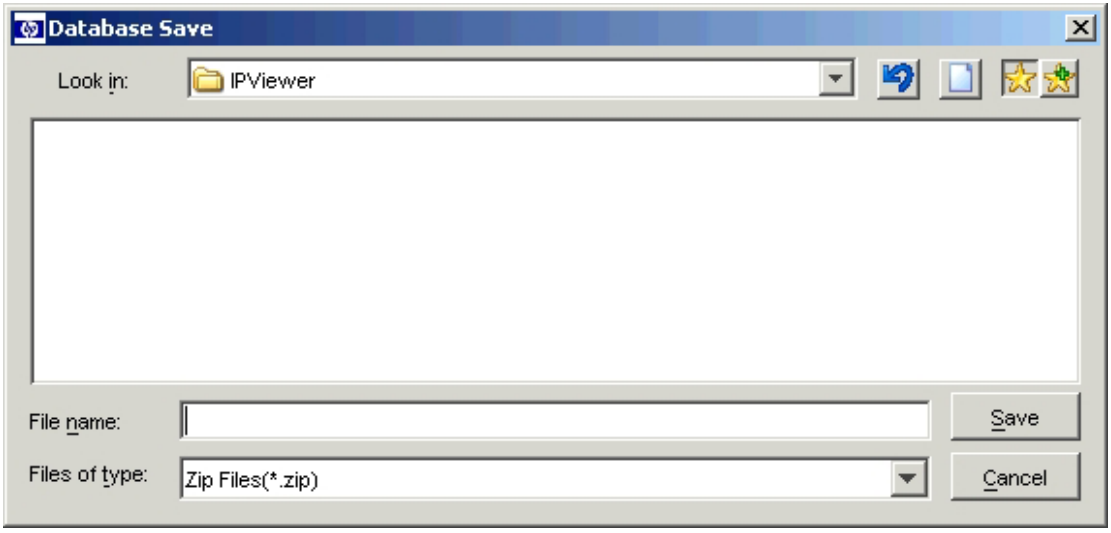

Figure 10-5: Database Save dialog box

2. Enter a file name, and browse to where the file is saved.
3. Click **Save.** A progress bar is displayed during the save. When finished, a message appears, indicating that the save was successful.

Exporting Local Databases

This function enables you to export fields from the local database to an ASCII comma-separated value (CSV) file or tab-separated value (TSV) file.

NOTE: The Address field only applies to console switches, and the Browser URL field only applies to servers. In the exported file, the Address field data is empty for servers and the Browser URL field data is empty for console switches.

To export a local database:

1. Select **File>Database>Export.** The Database Export dialog box appears.

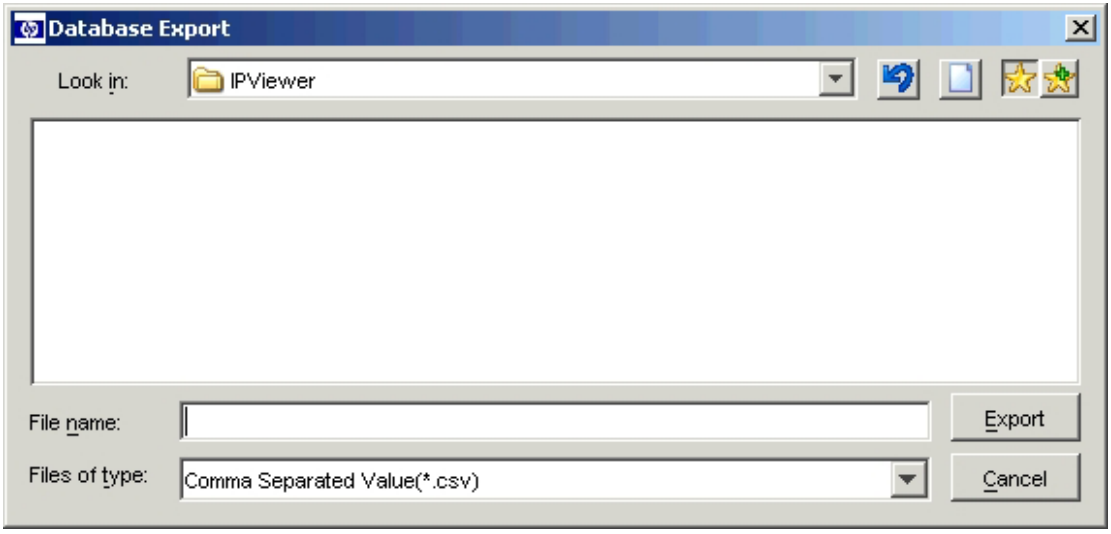

Figure 10-6: Database Export dialog box

2. Enter a file name in the Filename: field, and browse to the location where you want to save the exported file.
3. Select the type of export format from the Files of Type: dropdown list.
4. Click **Export.** A progress bar is displayed during the export. When finished, a message appears, indicating that the export was successful.

Loading Local Databases

This function enables you to load a database that was previously saved. While the database is being loaded, no other activity is allowed. All other windows, including Video Session Viewer and the Manage Console Switch windows, must be closed. If other windows are open, a message appears, prompting you to either continue, which closes all open windows, or quit, which cancels the database save progress.

To load a local database:

1. Select **File>Database>Load.** The Database Load dialog box appears.

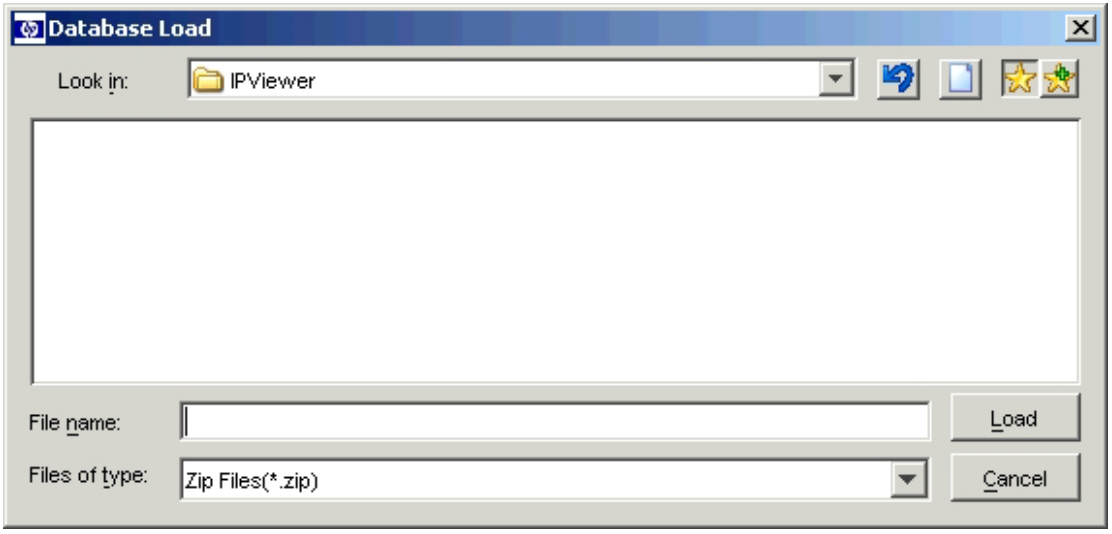

Figure 10-7: Database Load dialog box

2. Browse to select the database to load.
3. Click **Load.** A progress bar is displayed. When loading is finished, a message appears, indicating that the load was successful.

11

Troubleshooting

Problem	Solution
You cannot access any servers on the console switch after changing the IP address.	The IP address in the Network subcategory and under the console switch Properties window must match to have full functionality.
The LAN connection in the Diagnostic screen displays as green when the network cable has been disconnected from the console switch.	Wait one minute and recheck the status of the LAN connection in the Diagnostics screen.
You cannot select the checkbox in front of the type of Interface Adapters to upgrade.	The checkbox cannot be selected if all Interface Adapters have current firmware.
The dropdown lists under the console switch Properties window are empty.	The dropdown lists are empty until you enter more than one name for the selected category.
You attempt to launch the Video Session Viewer, and a black screen appears.	There is no communication from the server. • Be sure that the server is powered on. • Be sure that the power source is valid. • Be sure that the cables are connected properly.

continued

Problem	Solution
The display has a color streaking problem when the target server is running Windows XP, Windows 2000 (SP2), or Microsoft Windows NT® 4.0 (SP6).	Change the current resolution, 800 x 600 at 60 Hz, to 1024 x 768 at 60 Hz.
The local and remote cursors do not align.	Refer to Chapter 9.
You have intermittent Video Session Viewer issues.	• Click the **Align Local Cursor** icon in the Video Session Viewer. • Click **Tools>Automatic Video Adjust** in the Video Session Viewer.
The local and remote cursors do not align.	Click **Tools>Automatic Video Adjust** in the Video Session Viewer.
The user name and password are not accepted when you try to access Manage Console Switch.	If a new user name and password have not been created, the default user name is Admin (case-sensitive) and the default password field is blank.
The mouse cursor flickers.	The video driver does not properly support Direct Draw. Deselect the **Direct Draw** checkbox under Tools>Options.
The mouse leaves pixels changed.	Reduce the noise threshold to refresh smaller pixel quadrant changes.
The Discover Wizard does not discover console switches.	Erase the IP address in the From Address: and To Address: fields and enter the correct information.
Remote Insight Lights-Out Edition (RILOE) and Integrated Lights-Out (iLO) are not working correctly with the IP Console Switch system.	The HP IP Console Switch firmware must be version 2.0.6 or later.

continued

Problem	Solution
The Discover Wizard is taking a long time to scan a range of IP addresses.	It takes 4 seconds to scan each IP address. Enter a smaller range of IP addresses.
You get a login failure when LDAP is enabled.	Resolve the following: • The search credentials (DN and password) are not valid. • An invalid authentication mode (not basic, attribute, or group) is requested. • The group container cannot be found in the directory (Group Mode only). • The target computer can not be found (Group Mode only). You might also get this login failure, when the LDAP client cannot contact any LDAP server or DNS server.
After enabling Bootp (in the Settings Category) the Discover Wizard does not get an IP address or a random IP address is given.	The IP address must be statically assigned to the medium access control (MAC) address of the console switch. The Dynamic Host Configuration Protocol (DHCP) server must be enabled to respond to Bootp.
The Video Session Viewer is distorted when a Serial Interface Adapter is connected.	Click **Tools>Automatic Video Adjust** in the Video Session Viewer.

continued

Problem	Solution
You get an "Access cannot be granted due to Authentication Server errors" error when correct user name and password is used when using LDAP for authentication and authorization.	• Verify that the HP IP Console Switch or Interface Adapter is named exactly the same as in the LDAP directory. • Review the tutorial to gain a better understanding of LDAP functionality.
The Linux HP IP Viewer application is taking a while to start up.	• Verify that the loopback interface is up. • Verify that the /etc/hosts contains a 127.0.0.1 localhost entry.
SNMP Authentication Failure Traps are not being received.	The SNMP Authentication Failure Traps are turned off by default in Insight Manager. For more information, refer to the documentation included with HP Systems Insight Manager.

12

Upgrading Firmware Using TFTP

The HP IP Console Switch upgrade feature enables you to update the HP IP Console Switch with the latest available firmware.

To upgrade the HP IP Console Switch, you need a Trivial File Transfer Protocol (TFTP) service application on the workstation or server that will be used to perform upgrades. After the TFTP has been enabled, then upgrade the HP IP Console Switch firmware.

NOTE: The HP IP Console Switch 1x1x16 and HP IP Console Switch 3x1x16 with firmware 3.0.0 or higher cannot be downgraded to versions lower than 3.0.0. Any attempt to downgrade to versions lower than 3.0.0 will be rejected by the HP IP Console Switch.

TFTP for Windows Operating Systems

Follow the instructions in the \TFTP\TFTP Install Instructions.txt file on the CD included with this kit or the Softpaq TFTP directory.

TFTP for Linux Operating Systems

For most systems using Red Hat Package Manager (RPM) packages, TFTP is provided by the TFTP server RPM (RPM-IVH/Redhat/RPMS/). Depending on the type of distribution, the Internet services daemon is provided by xinetd.

NOTE: The following Linux example uses Red Hat 3.0. For more information, refer to your Linux operating systems HELP, or documentation.

NOTE: By default, TFTP executes in secure mode and only provides readable files under the /tftpboot directory. Other directories can be specified through the /etc/xinetd.d/tftp files. In secure mode, TFTP expects the file to be relative to the /tftpboot directory.

To enable TFTP for Linux operating systems (GNOME):

1. Go to the main menu, and select **Programs>System>Service Configuration.**
2. In the Service Configuration menu, verify that the xinetd checkbox is selected to start at boot.

   -or-

   If the checkbox is not selected, select the checkbox and click **Save.**
3. Find TFTP in the list of services and highlight it.
4. Select the checkbox to start TFTP at boot, then click **Save.**

To enable TFTP for Linux operating systems (KDE):

1. Go to the main menu, and select **Control Panel>Services.**
2. In the Service Configuration menu, verify that the xinetd checkbox is selected to start at boot.

   -or-

If the checkbox is not selected, select the checkbox and click **Save.**

3. Find TFTP in the list of services and highlight it.
4. Select the checkbox to start TFTP at boot, then click **Save.**

Verifying TFTP for Linux Operating Systems

NOTE: The following Linux example uses Red Hat 3.0. For more information, refer to your Linux operating systems HELP, or documentation.

1. Verify that `in.tftpd` service is running with the following `ps -ef | grep tftpd`.

   By default, the `/etc/xinetd.d/tftp` configuration file uses `/tftpboot` as the directory.
2. Create a `/tftpboot` directory, if it does not exist, and set the permissions for public access.
3. Copy the firmware file to `/tftpboot`.
4. Cd to `/tmp`.
5. From a shell prompt, enter `tftp localhost` (or name of local system).
6. Download the file by entering the following command:

   ```
   get /tftpboot/filename
   ```
7. Enter `quit`.
8. From the shell prompt, verify that the file is in the `/tmp` directory.

If the TFTP was configured correctly, the preceding steps should transfer the file to the current directory.

Upgrading the HP IP Console Switch Firmware

Before beginning the upgrade procedure, be sure that the Secure TFTP Server is installed and that the GET access permissions for the folder the updated file is in is selected. Also, be sure that the HP IP Console Switch is on the same network as the computer that is being used for the upgrade.

Windows Operating Systems

To upgrade the firmware on Windows operating systems, follow the instructions in the \TFTP\TFTP Install Instructions.txt file on the CD included with this kit or the Softpaq TFTP directory.

Linux Operating Systems

NOTE: The following Linux example uses Red Hat 3.0. For more information, refer to your Linux operating systems HELP, or documentation.

To upgrade the firmware on Linux operating systems:

1. Connect one end of a serial cable to an available COM port on the server or workstation.
2. Connect the other end of the above serial cable to the serial port on the HP IP Console Switch.
3. Configure the terminal emulation software for the server, such as Minicom.

   To configure Minicom:

   IMPORTANT: Minicom is a utility that is loaded during the installation of Linux. However, if you do not select the option to install the Linux Utilities during the operating system installation, you cannot use Minicom without downloading the Minicom X.X..i386.rpm file from the Red Hat website. (Refer to the procedure for installing RPMs from the Red Hat website.)

   a. Log on to a Linux console, or open a terminal and enter "minicom-s" at the command prompt. The Configuration menu appears.

   b. Select **Serial Port Setup.** The Change which setting? menu appears.

   c. Select **Option A (Serial Device).** Manually change the device type from "dev/modem" to "/dev/ttyS0," and press the **Enter** key.

   d. Select **Option E (Bps/Par/Bits).** The Comm Parameters menu appears.

   e. Select **E (Speed 9600 Bps),** and press the **Enter** key. The designation 9600 8N1 appears next to Option E.

f. Select **Option F (Hardware Flow Control).**

   Be sure that the Change which setting? menu looks as follows:

   A—Serial Device: /dev/ttyS0

   B—Lockfile Location: /var/lock

   C—Callin Program:

   D—Callout Program:

   E—Bps/Par/Bits: 9600 8N1

   F—Hardware Flow Control: No

   G—Software Flow Control: No

g. Press the **Enter** key to return to the Configuration menu. Scroll down to the **Save setup as dfl** option, and press the **Enter** key.

h. Scroll down the Configuration menu to the Exit from Minicom option, and press the **Enter** key.

i. From the Linux command prompt, enter `minicom`. As soon as a connection is established, the Main menu for the HP IP Console Switch appears. Follow the on-screen options to configure the HP IP Console Switch. The IPViewer HyperTerminal menu with six options appears.

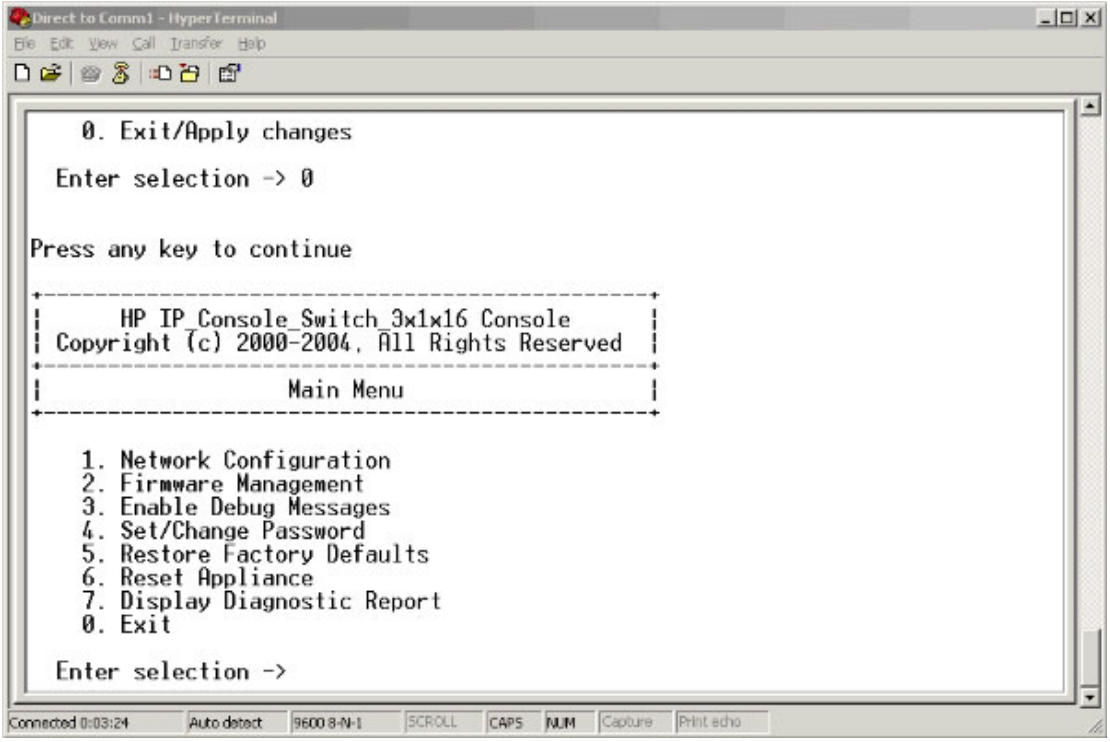

Figure 12-1: HP IP Viewer HyperTerminal menu

4. Plug the supplied power cord into the rear of the HP IP Console Switch and then into a valid power source, if not already connected.
5. Power on the HP IP Console Switch, if not already powered on. The activity indicator on the rear panel powers on. The activity indicator blinks for 30 seconds while performing a self-test. Approximately 10 seconds after it stops blinking, press the **Enter** key to access the main menu.

6. Select **Option 2—Firmware Management.** The Firmware Management menu appears.

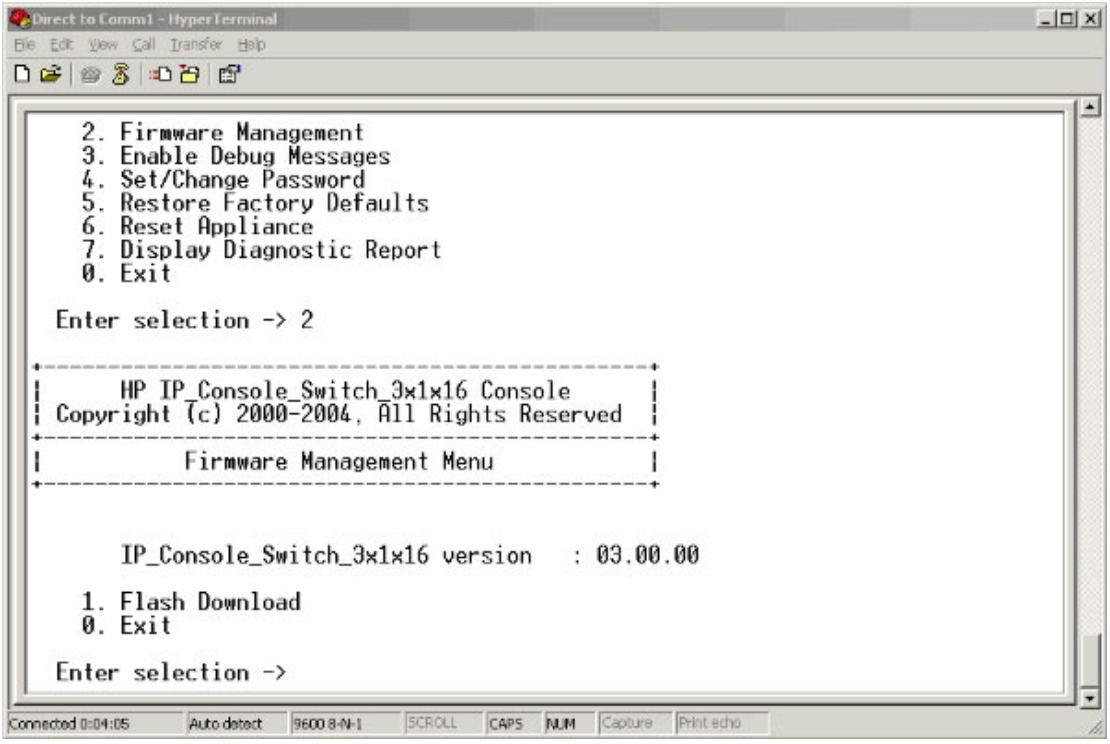

Figure 12-2: Firmware Management menu

7. Select **Option 1—Flash Download.**

8. Enter the IP address of the TFTP server that has the updated file and the exact path of the updated file (for example, C:\tftp\h3_0_0_english.fl).

9. Enter **Y** at the prompt to download the upgrade file from the given IP address. The HP IP Console Switch begins upgrading.

CAUTION: Do not cycle power to the HP IP Console Switch during this process. A loss of power might render the HP IP Console Switch inoperable and require that the unit be returned to the factory for repair. The update can take as long as 10 minutes.

When the upgrading process is complete, the HP IP Console Switch reboots. The HP IP Console Switch is ready.

Upgrading the HP IP Console Switch Firmware through the HP IP Console Viewer

Follow the instructions in the \TFTP\TFTP Install Instructions.txt file on the CD included with this kit or the Softpaq TFTP directory.

A

HP IP Console Switch Directory Service Setup

This document is intended as a tutorial to familiarize you with the LDAP directory functionality of the HP IP Console Switch. It walks you through the steps to set up an HP IP Console Switch to work with a Microsoft Active Directory server in group attribute mode, in which users, Interface Adapters, and HP IP Console Switches are members of the same group, and authenticate only mode, in which the directory is used only to validate the user and access controls managed in the HP IP Console Switch. A mode to use for testing communications with the directory server is explained as well.

NOTE: The reader is expected to understand the concepts of LDAP directories and how to use Microsoft Active Directory tools. This document is not intended to explain LDAP directories.

Hardware Configuration Used for This Example

- HP IP Console Switch
- Windows 2003 Server Domain Controller
- Windows 2003 Server running HP IP Console Viewer application
- Servers connected to the HP IP Console Switch as target systems

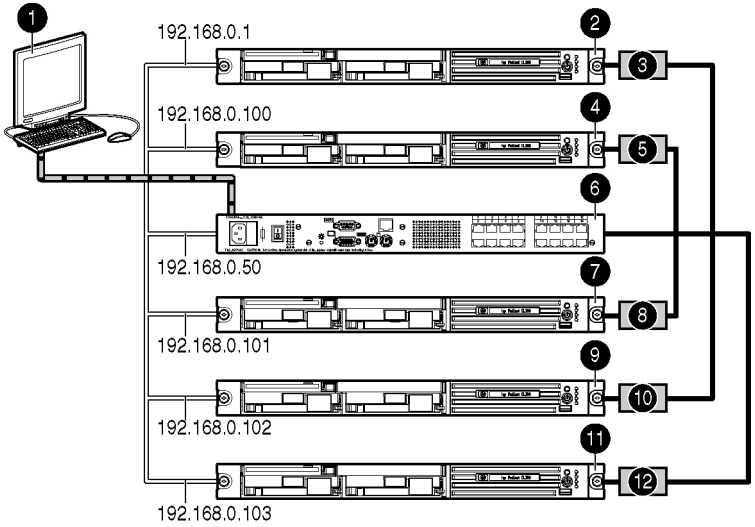

Figure A-1: LDAP Hardware Configuration

Item	Description
1	Keyboard, video display and mouse
2	Windows 2003 Server Domain Controller (Widget-AD)
3	Interface Adapter (Widget-AD-IA)
4	Server (Brahms)
5	Interface Adapter (Brahms)
6	HP IP Console Switch (Rack-10-KVM)
7	Server (Handel)
8	Interface Adapter (Handel)
9	Server (Bach)
10	Interface Adapter (Bach)
11	Windows 2003 Server HP IP Viewer (Vivaldi)
12	Interface Adapter (Vivaldi)

Setting Used for This Example

- The Microsoft domain controller acts as the DHCP server and DNS server in these examples.
- The domain is widget.com.
- The user account that is used to query the domain controller for authentication and access controls is kvmquery.
- The OU for grouping HP IP Console Switches and users is KVMLDAP.

Authentication and Group-Level Access Controls

This procedure gives an example of how to use Active Directory for authentication and group-level access controls.

1. Name the Interface Adapters to match exactly the names of the computers with which they are connected. This must be done using the OSD from the local port PS/2 and video connectors. The domain controllers Interface Adapter should have a different name than the domain controller. A computer with the same name representing the domain controller should be added separately to the directory for IP console access because the domain controllers are not listed under computers in the Active Directory.

   In this example, the Interface Adapter for the domain controller Widget-AD is named Widget-AD-IA, and a computer is created with the name Widget-AD-IA. A standard user cannot authenticate for a domain controller. However, the default user administrator can.

   To name Interface Adapters:

   a. From the local OSD, press the **Print Scrn** key. The Main dialog box appears.

Figure A-2: Main dialog box

b. Click **Setup>Names.** The Names dialog box appears.

c. Click the name you want to change, and click **Modify** and then **OK.**

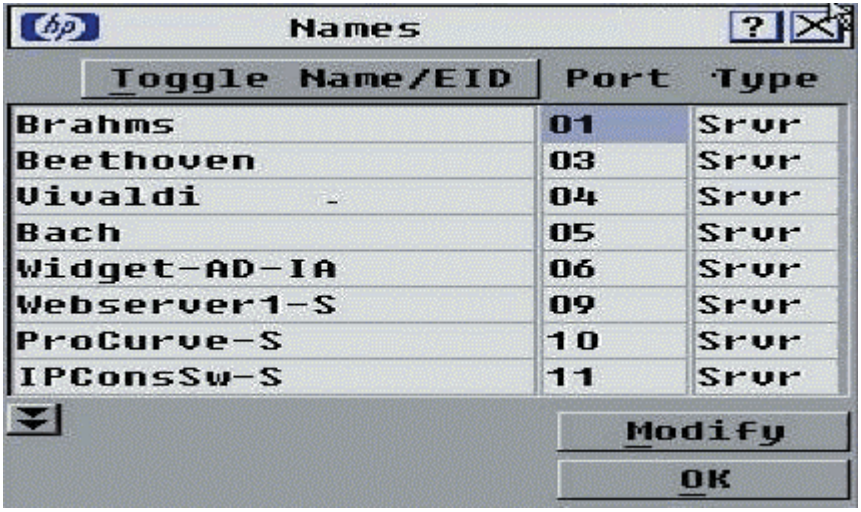

Figure A-3: Names dialog box

2. Install and launch the HP IP Console Viewer application on a Windows workstation that has network connectivity to the HP IP Console Switch.

3. Discover or manually add the console switch. For information on how to manually add or discover console switches, refer to Chapter 4, "Adding and Discovering Console Switches."
4. Access the console switch and log in as admin with no password or with the admin-level user name and password of your console switch. For information on how to access the console switch, refer to Chapter 5, "Accessing Console Switches."
5. Name the HP IP Console switches from the HP IP Console Viewer using the Manage Console Switch window.

IMPORTANT: The HP IP Console Switch names must always be synchronized with the names used for associated computer account objects in the directory LDAP Directory Service. It is also important to note that Active Directory (AD) allows multiple computer accounts to have the exact same name, as long as each account is in a different domain from the others. When using the Group query mode, it is important to have precisely one account for each console switch and precisely one account for each attached server. If multiple accounts in the AD forest are allowed to have the same name, unexpected failures may occur when using the Group query mode.

6. Select the **SNMP** subcategory to view or change the console switch name. This name is displayed on the Authentication subcategory.

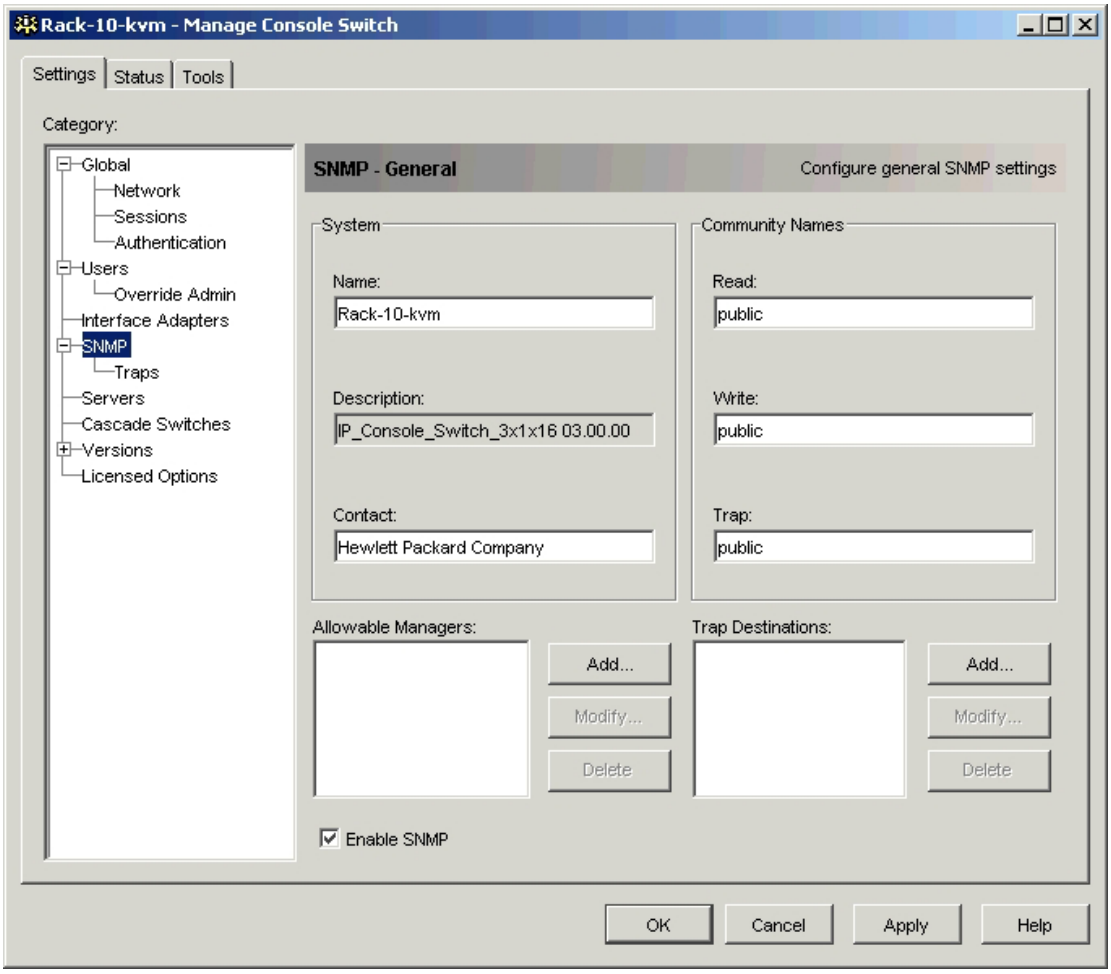

Figure A-4: SNMP subcategory

7. Add the license key on the HP IP Console Switch from the HP IP Console Viewer application. For information, refer to the "Purchasing License Keys" and "Enabling Directory Services Integration" in chapter 7 of this guide.

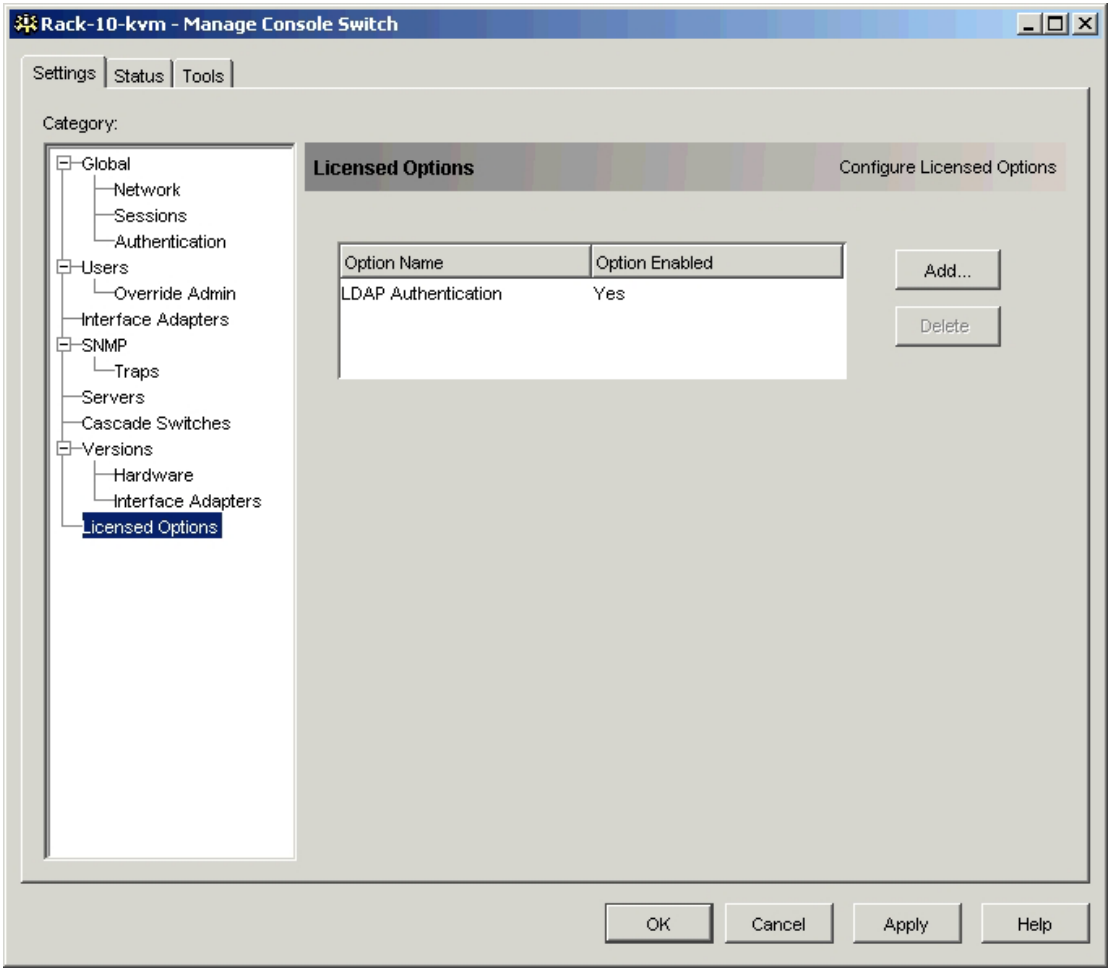

Figure A-5: License Options category

8. Expand the Global category, and select the **Authentication** subcategory.

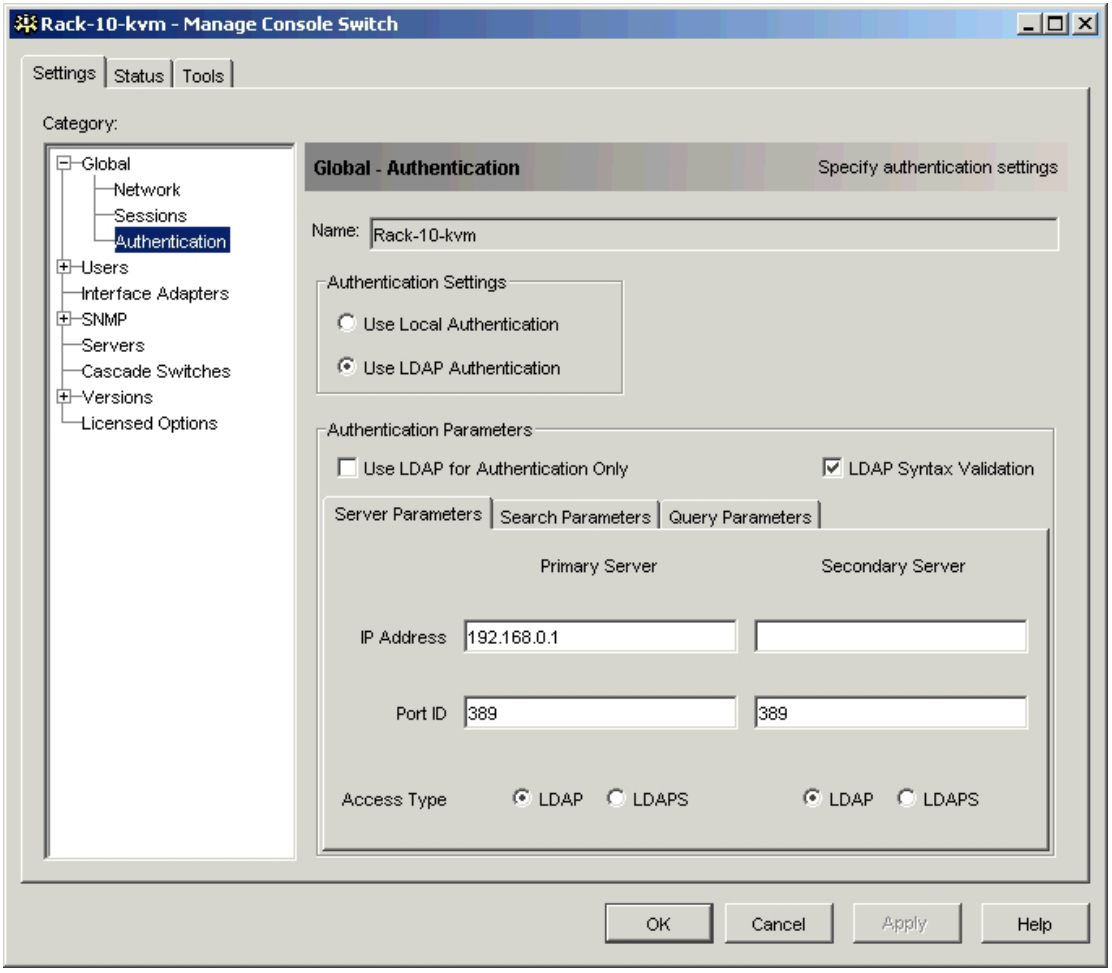

Figure A-6: Authentication subcategory

9. Enable LDAP on the HP IP Console Switch.
   a. Click **Use LDAP Authentication.**
   b. On the Server Parameters tab, enter the IP address of the **Primary Server** (domain controller).

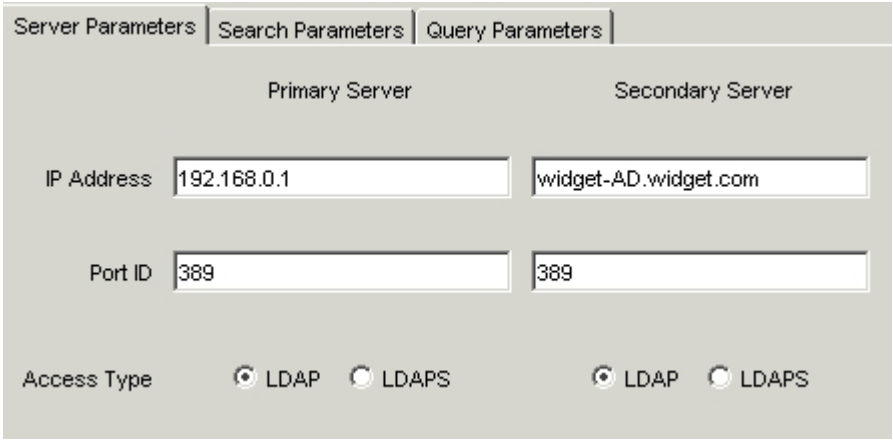

Figure A-7: Server Parameters tab

   c. On the Search Parameters tab, enter the Search DN cn=kvmquery,cn=users,dc=widget,dc=com.

NOTE: The first cn field must match the full name of the user, not the login name. For example, if the user name is John Doe, then *cn=John Doe* (note the space in the name).

   d. Enter the search password for the kvmquery user account.
   e. Enter the search base dc=widget,dc=com.

NOTE: The search base should always be at the root of the domain.

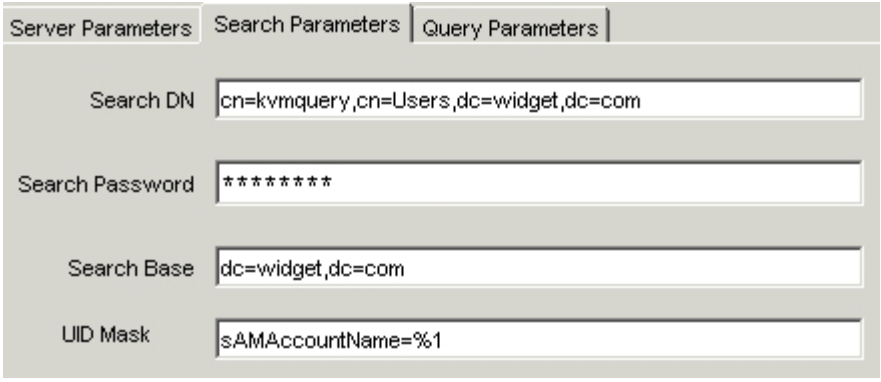

Figure A-8: Search Parameters tab

f. On the Query Parameters tab, click **Basic** for Query Mode (Console Switch) and **Basic** for Query Mode (Server).

g. Apply the settings.

NOTE: This query mode is used for testing and troubleshooting, but it should not be used in a production environment. After the basic LDAP communications are tested successfully, change the query mode.

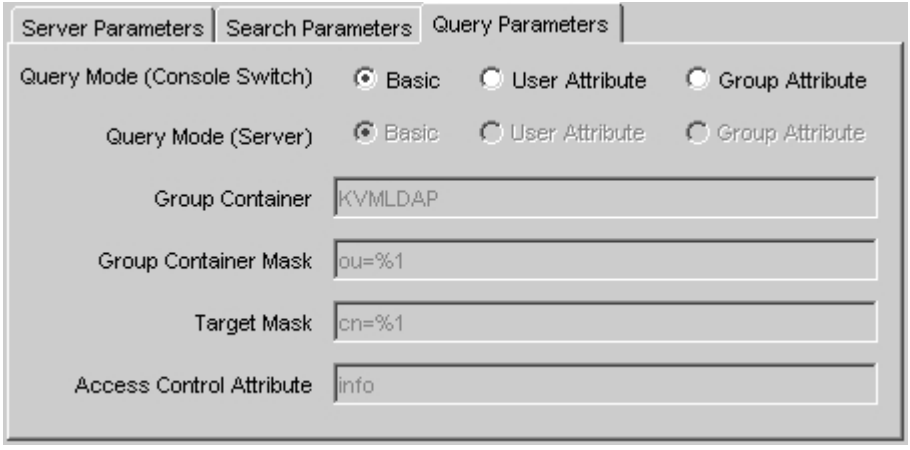

Figure A-9: Query Parameters tab

NOTE: In a production environment, work with your IT department to create the kvmquery user account and add the KVMLDAP IP console switch OU. You need a level of access that enables you to create, delete, modify groups, and add computer objects for Interface Adapters connected to non-domain systems within the IP console switch OU. Use the Microsoft MMC to access the Active Directory from another server or a client workstation.

To administer the directory from the domain controller console, click **Start>Programs>Administrative Tools>Active Directory Users and Computers.**

-or-

To use MMC from another Windows 2003 server:

1. Click **Start>Run>enter MMC.**
2. From MMC, click **File>Add/Remove Snap-in.**
3. Add **Active Directory Users and Computers.**
4. Close **Add/Remove Snap-in** and click **OK.**
5. From Active Directory Users and Computers, highlight **Add Users and Computers.**
6. Click **Action>Connect to Domain.** The domain list appears.

10. On the domain controller, add an OU group container named KVMLDAP to Active Directory for the HP IP Console Switches, users, Interface Adapters, and groups to be placed in the KVMLDAP OU.
    a. Right-click **widget.com.**
    b. Choose **New Organizational Unit.**
    c. Name it KVMLDAP.
    d. Click **OK.**

NOTE: When using the Group Query Mode, the OU object used as the Group Container must be located in the domain that is used as the Search Base. The Relative Distinguished Name of the Group Container is configured in the Group Container field of the Authentication subcategory. The Distinguished Name of the Search Base is also configured in the Authentication subcategory. If the Group Container is located outside the domain used as the Search Base, all attempts to launch a KVM Session or to manage a console switch fails.

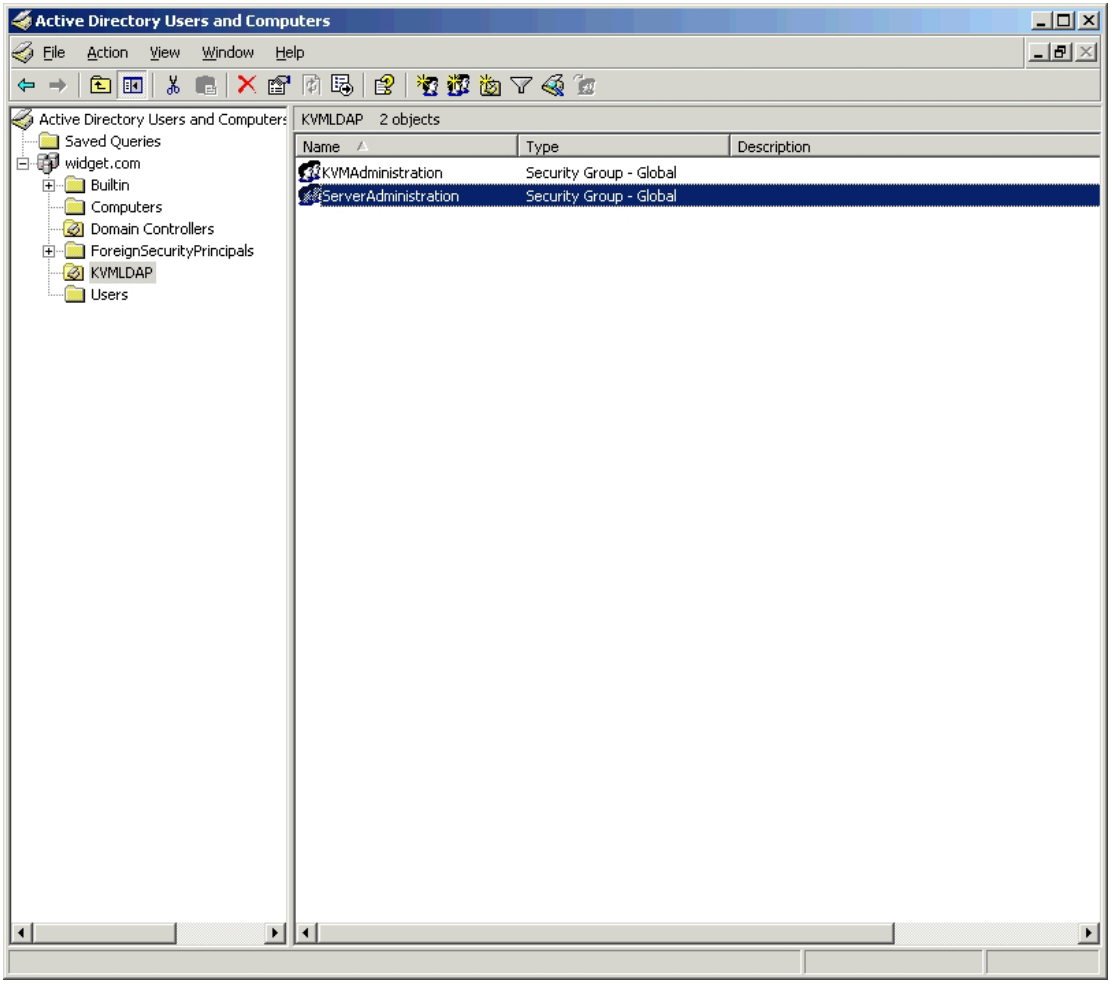

Figure A-10: Active Directory Users and Computers

11. Create a user named KVMQUERY, and assign a password.
    a. Click **User>New>User.**
    b. Follow the wizard.
    c. Set the password to not expire.
    d. Click **Finish.**

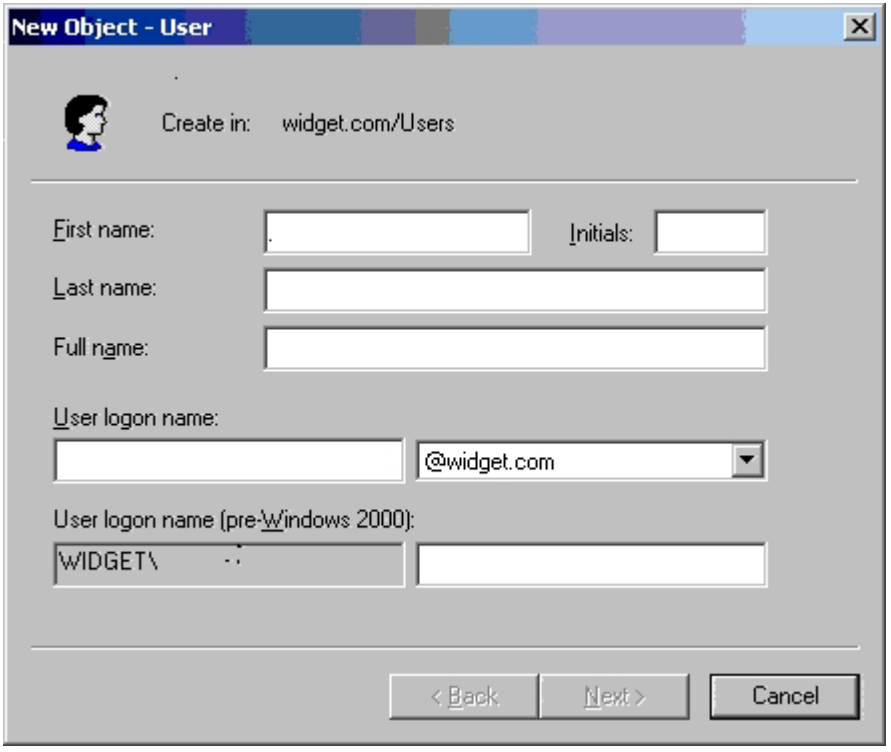

Figure A-11: New Object—User dialog box

12. Create two groups for HP IP Console Switch administrators and users.
    a. Right-click **KVMLDAP OU.**
    b. Choose **New Group.**
    c. Create groups named KVMAdministration and ServerAdministration.

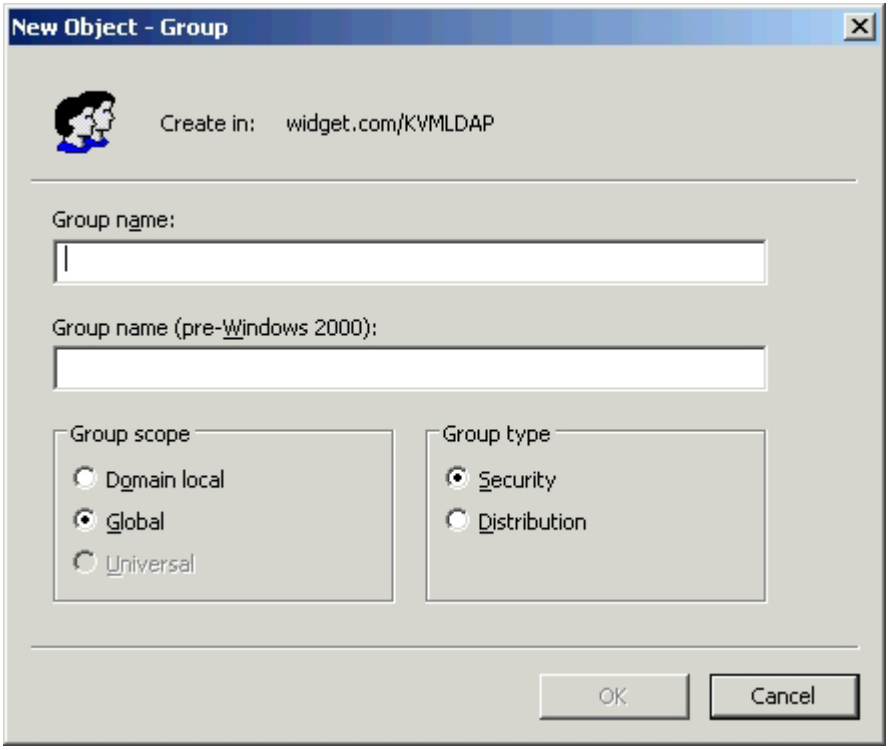

Figure A-12: New Object—Group dialog box

NOTE: In a production environment, groups in Active Directory IP console switch OU would match the organization's hierarchy, usually by function, geography, or a combination.

Set up the default access control for the KVM Access group by right-clicking Properties for the group and entering `KVM User` in the group's notes field.

Setup the default access control for the KVM Administration group by right-clicking Properties for the group and entering `KVM Appliance Admin` in the group's notes field.

13. Add the users and Interface Adapters to the appropriate groups that associate them.
    a. Right-click each of the two new groups.
    b. Click **Properties.**
    c. Select the **Members tab.**
    d. Click **Add.**
    e. Click **Object Types.**
    f. Select **Computers and Users.**
    g. Click **OK.**
    h. Click **Advanced>Find Now.**
    i. Add the computer and users that should belong together in the group by clicking the first object holding the control key while clicking the others.
    j. Click **OK.**

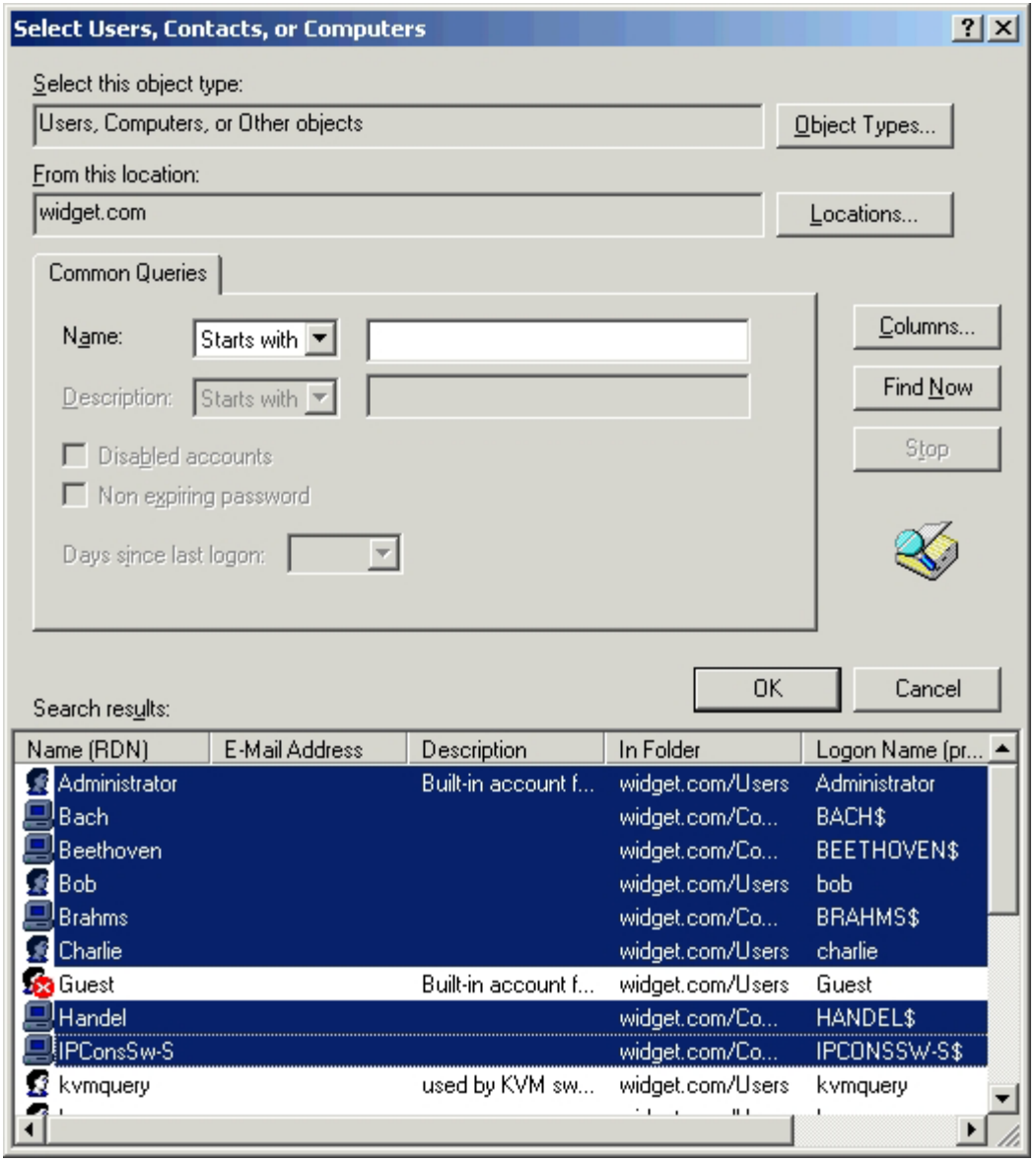

Figure A-13: Select Users, Contacts, or Computers window

14. From HP IP Console Viewer application, log in to the HP IP Console Switch from the HP IP Console Viewer application.

    a. Click **Global>Authentication.**

    b. On the Query Parameters tab, click **Basic for Query Mode (Console Switch)** and **Basic for Query Mode (Server).**

    IMPORTANT: This query mode should be used in a production test environment. After the basic LDAP communications configuration is successfully tested, change the query mode because Basic mode gives full administrative authorization to all console switches and all attached servers.

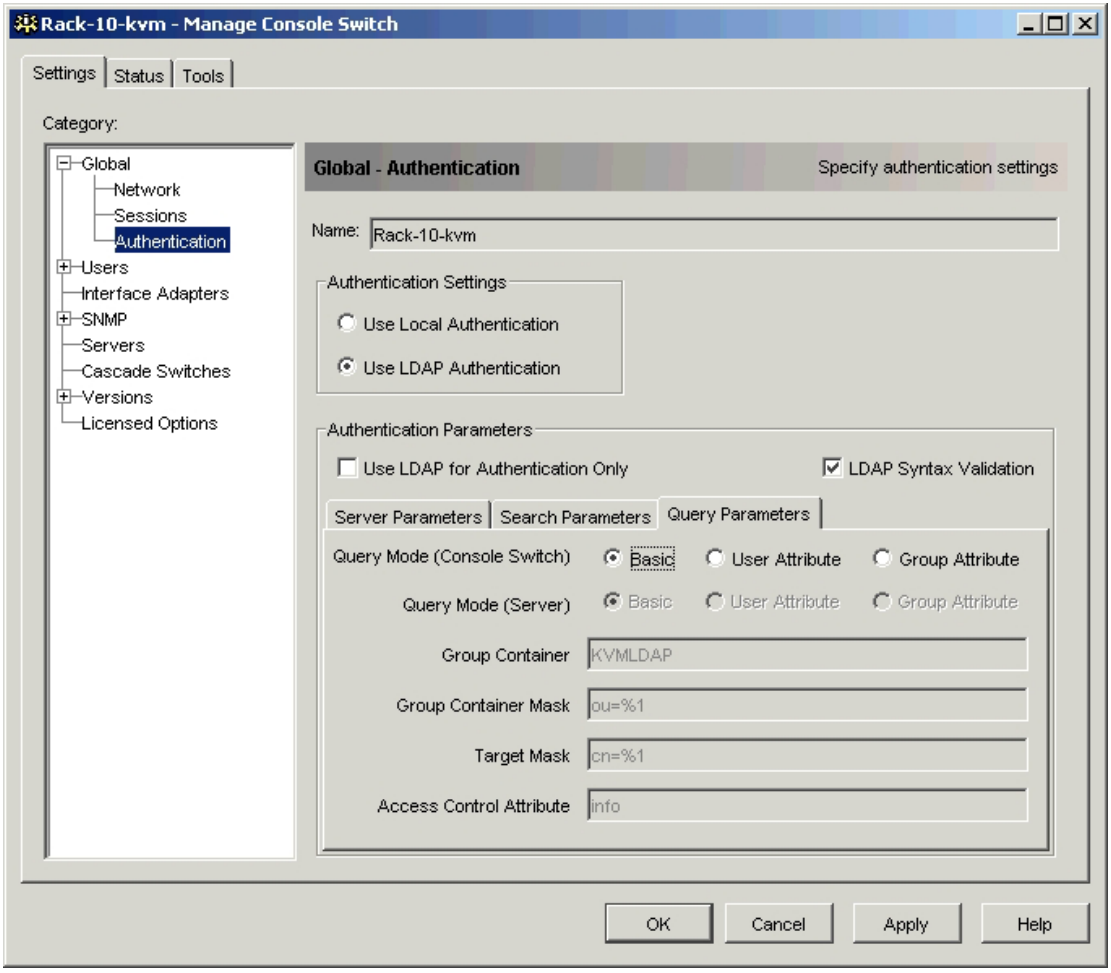

Figure A-14: Authentication subcategory

15. Test the LDAP communications from the HP IP Console Viewer application.

    a. Click **Tools>Clear Login Credentials.**

    IMPORTANT: Perform this step each time you want to test authentication of a user to a target system.

b. Choose a server previously added to the directory as a computer to one of the groups, and log in as a user from the same group.

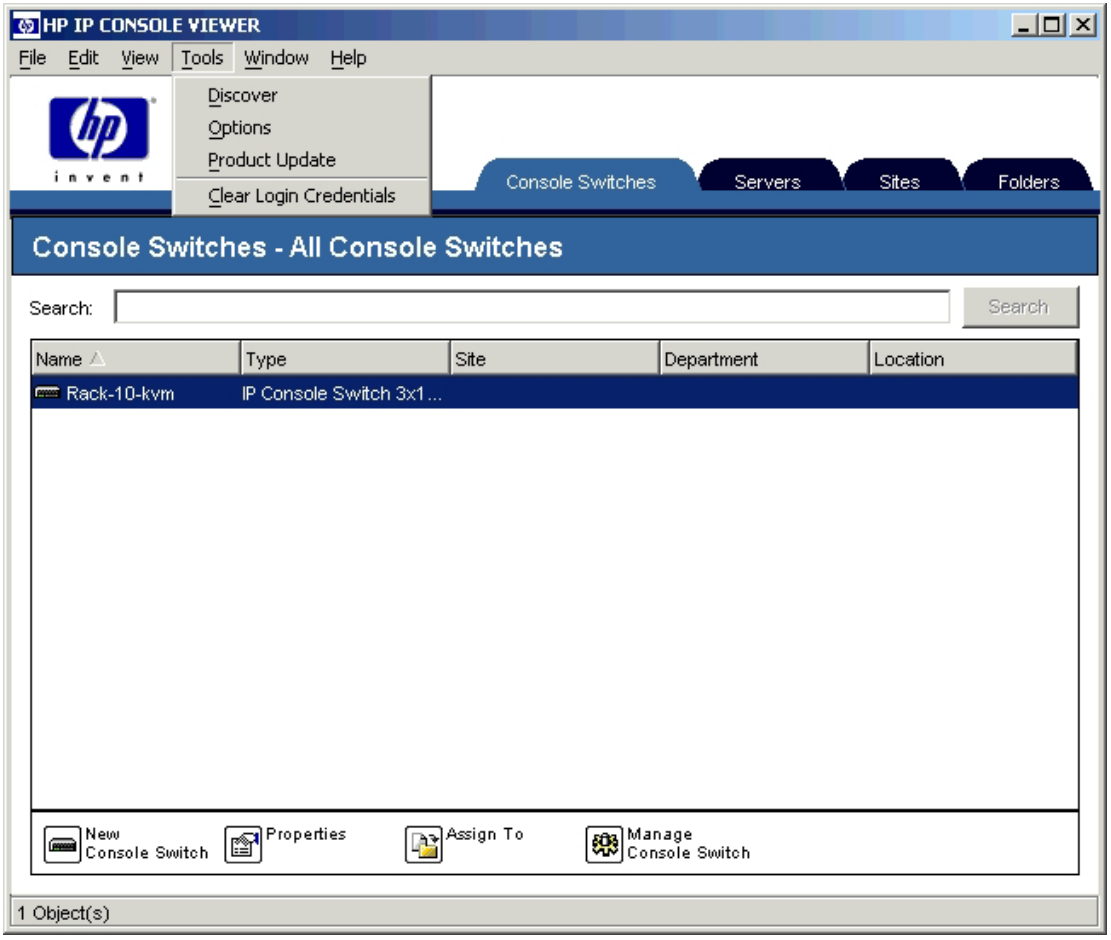

Figure A-15: HP IP Console Viewer main window

16. After the basic LDAP communication test succeeds, log in to the HP IP Console Switch from the HP IP Console Viewer application.

    a. Click **Global>Authentication.**

b. On the Query Parameters tab, click **Group Attribute for Query Mode (Console Switch)** and **Group Attribute for Query Mode (Server).**

c. Enter the **Group Container KVMLDAP.**

d. Apply the settings.

e. Test again.

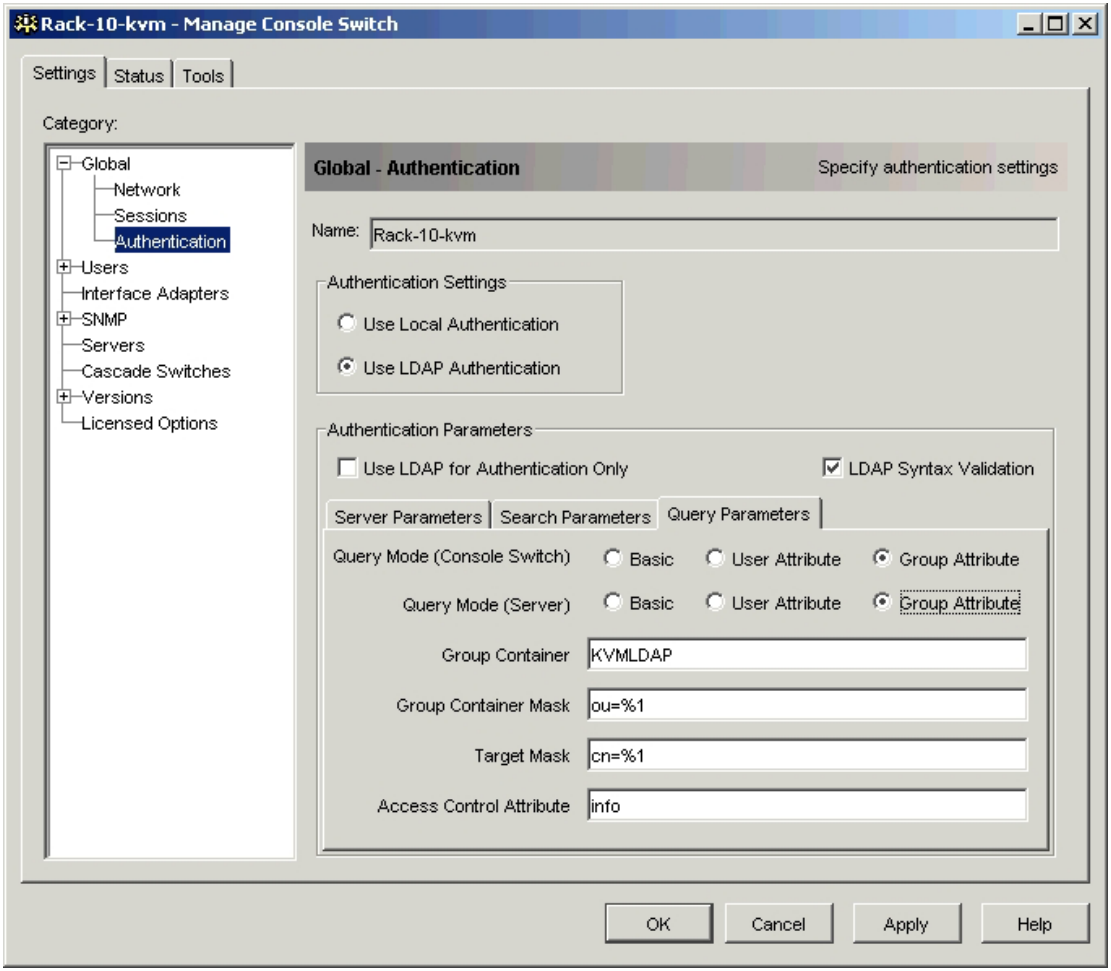

Figure A-16: Authentication subcategory

Authentication Only

This procedure gives an example of how to use Active Directory for authentication only.

1. Follow the preceding steps 2–10.
2. Create user accounts locally in the HP IP Console Switch.

   IMPORTANT: The HP IP Console Switch user names must match exactly with their full display names in Active Directory.

3. Enable LDAP on the HP IP Console Switch.
4. Create user accounts locally in the HP IP Console Switch.

   IMPORTANT: The HP IP Console Switch user names must match exactly with their full display names in Active Directory.

5. Set the user's access controls locally on the HP IP Console Switch.
6. Test the LDAP communications from the HP IP Console Viewer application.
7. Click **Tools>Clear Login Credentials.**

   IMPORTANT: Perform this step each time you want to test authentication of a user to a target system.

8. After the basic LDAP communication test succeeds, log in to the HP IP Console Switch from the HP IP Console Viewer application.
   a. Click **Global>Authentication.**
   b. Check **Use LDAP for Authentication Only.** The fields on the Query Parameters tab are deactivated when this box is selected.

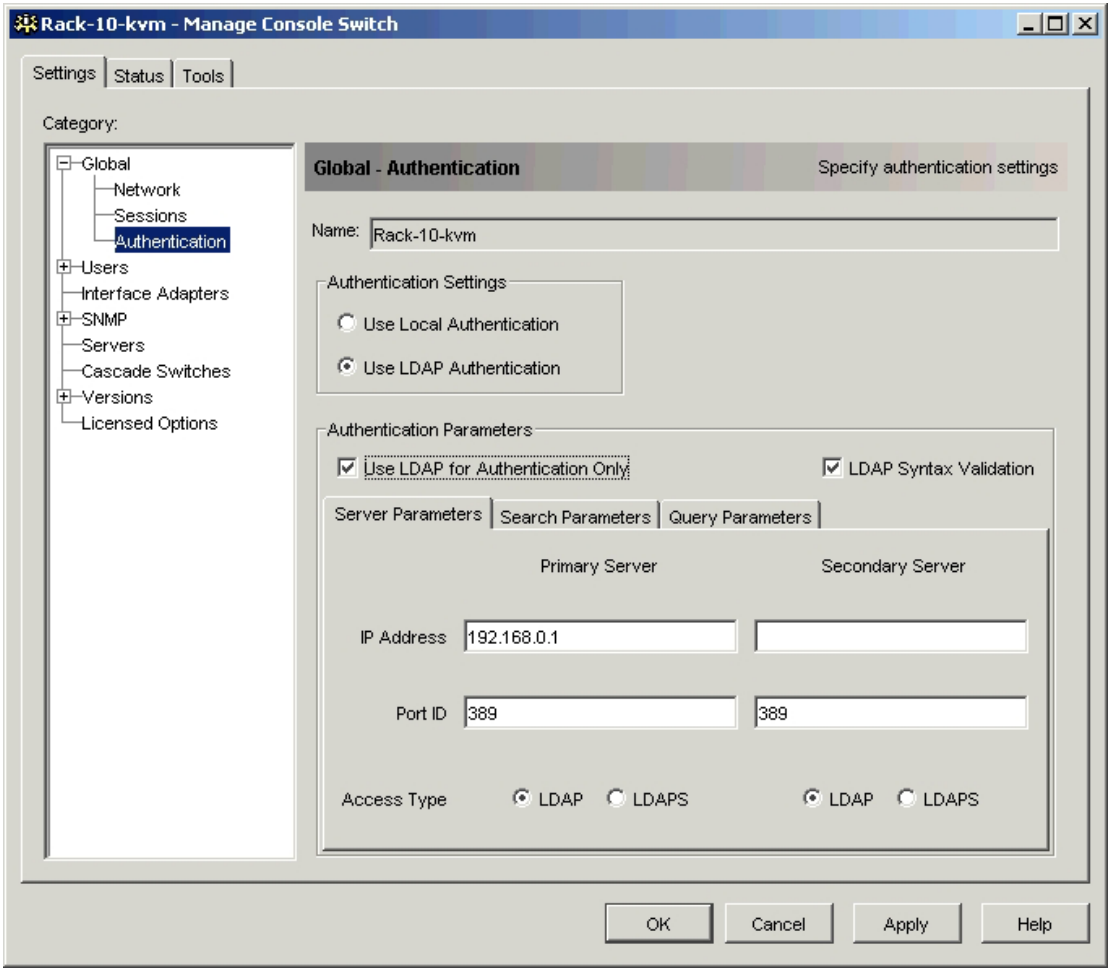

Figure A-17: Authentication subcategory

9. Apply the settings.
10. Test again.

B

LDAP Client Behavior

UID Masks (Simple and Complex)

The client application login dialog enables you to enter two fields, labeled User name and Password. Before the HP IP Console Viewer application was enhanced with support for Directory Services Integration (LDAP), the product supported only one form of authentication, which used an internal database. Therefore, there was no ambiguity about the use of these two fields because the internal database supports only one form of user name. However, Active Directory (AD) supports many types of attributes that could sensibly be used as credentials for the purposes of authenticating the user of the client application. After an administrator chooses which AD attributes to use as credentials, the choice is implemented using a feature of the HP IP Console Switch called the UID Mask. This flexibility engenders several questions:

- What are the AD attributes that could sensibly be used as credentials?
- How does the value of each of those attributes get set in AD?
- How is the UID mask in the MP used to implement a customer's choice of credentials?

These questions are addressed in the following subsections.

AD Attributes That May Be Used as Credentials

Several attributes that are candidates for use as credentials are defined when a new user account is initialized in AD. Other candidates are found in the Properties dialog for user objects in AD. In addition, other candidates are available but not readily accessible in the default Properties dialog for user objects. For these attributes, it is necessary to use an AD tool, such as ADSI Editor, to access the attribute and set its value.

Attributes Initialized During Creation of a New User Object

When a new object is created in AD to represent a user, the dialog presented by AD enables values to be set for the following attribute types:

- First Name
- Initials
- Last Name
- Full Name
- User Logon Name
- User Principal Name

  NOTE: This attribute is not explicitly labeled in the dialog used to create a new user object.

- User Logon Name (pre-Windows 2000)

When a new object is created, the values entered for each of these fields is stored in a specific attribute type within the object. In some cases, a value gets stored in more than one attribute. Some of the values are subsequently available for viewing and modification in the Properties dialog. The following table shows these relationships as well as others.

Table B-1: AD Attributes That May Be Used as Credentials

Field Label in New Object-User Dialog	Field Label in User Properties	AD Attribute Type	Comments
First Name	First Name	givenName	
Initials	Initials	initials	
Last Name	Last Name	sn	sn stands for surname.
Full Name	Display Name	DisplayName cn	The full name is stored in two AD attributes: displayName and cn. cn is abbreviation for Common Name.

continued

Table B-1: AD Attributes That May Be Used as Credentials *continued*

Field Label in New Object-User Dialog	Field Label in User Properties	AD Attribute Type	Comments
User Logon Name	User Logon Name	sAMAccount Name	This name is also used in pre-Windows 2000 logon name. However, the pre-Windows 2000 logon name might not be stored as an attribute, depending on the mode used to create the AD domain (Native mode versus Mixed mode).
Displayed but not labeled	Displayed but not labeled	userPrincipal Name	The default value for the UPN attribute has the form: <sAMAccountName>@<domain> This default value can be modified by replacing the sAMAccountName with any string of alphanumeric characters and can include: • Period (.) • Forward slash (/) • Backward slash (\) • Pound (#) • Dollar ($) • Hat (^) • Horizontal bar (|) • Minus (-) • Plus (+) The default domain can also be replaced with the name of any domain that is superior to the domain in which the object is being created.
- - - - -	E-mail	mail	
- - - - -	- - - - -	employeeID	Accessed by LDAP tool, such as ADSI Editor.

As an example, consider the following instance of the New Object–User dialog.

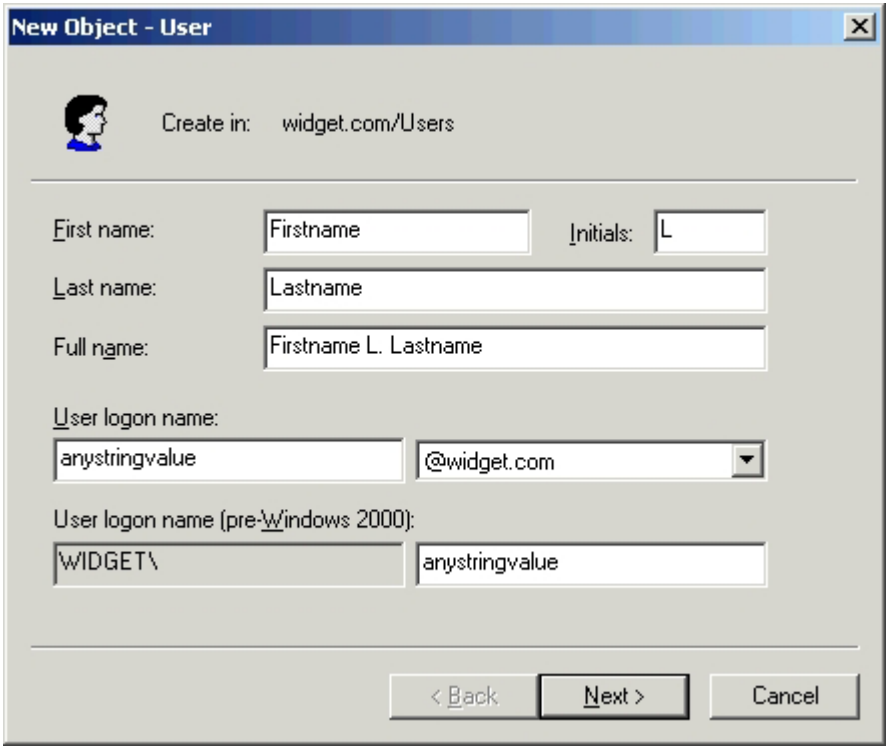

Figure B-1: New User-Object

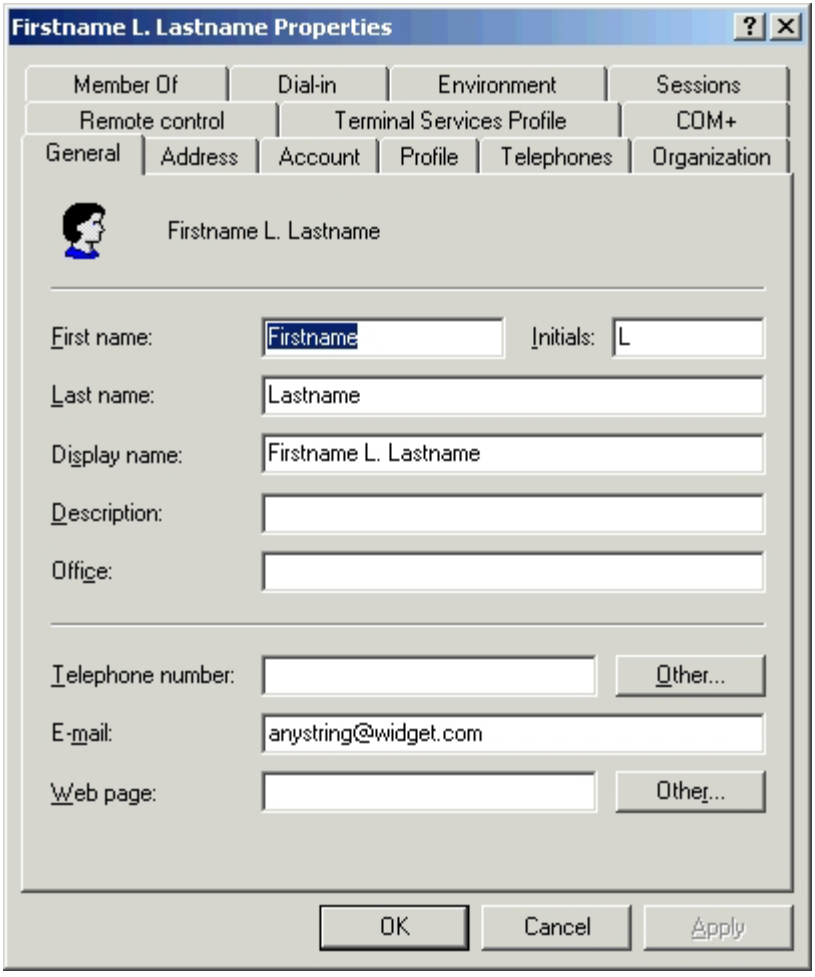

Figure B-2: Firstname L. Lastname Properties

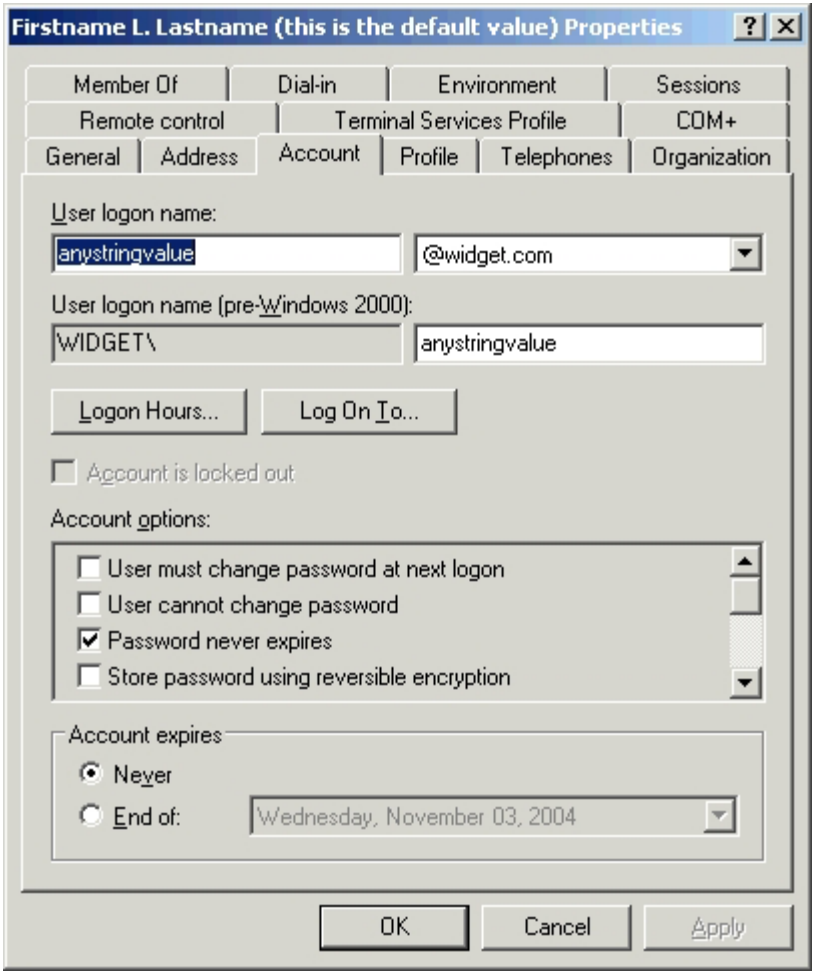

Figure B-3: Firstname L. Lastname Properties

Additional Attributes Available in User Properties

In addition to the Properties that are set during object creation, there is at least one property that could potentially be useful as a credential: E-mail.

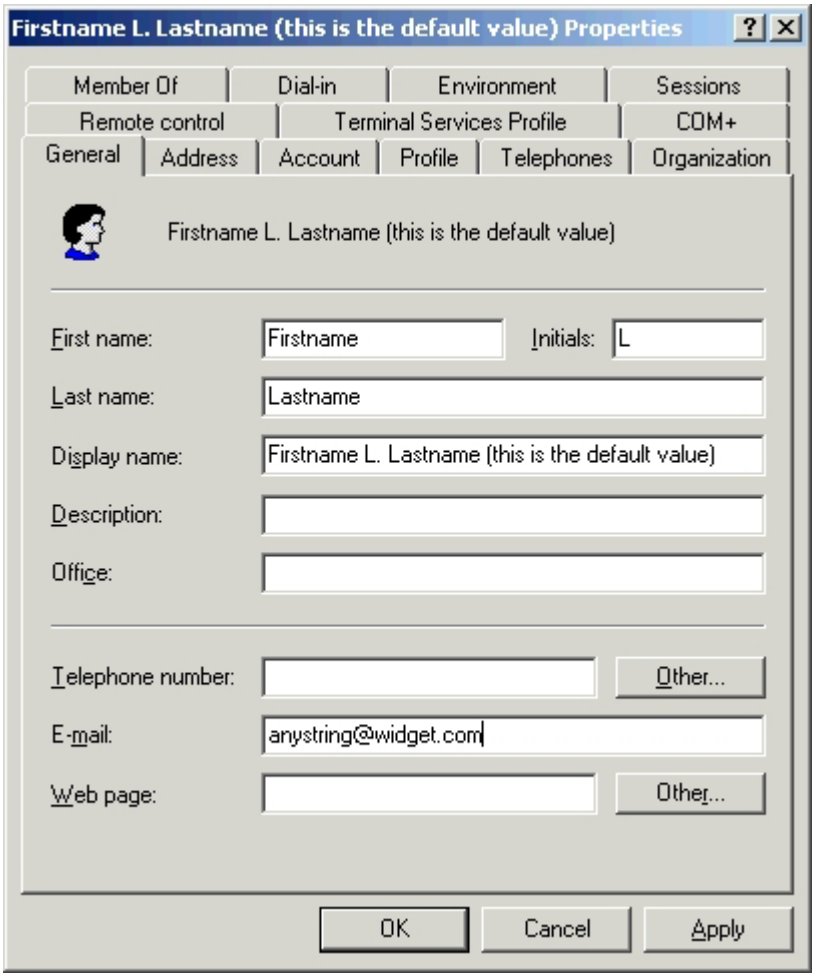

Figure B-4: Firstname L. Lastname

Additional Attributes Available through the ADSI Editor

In addition to the attributes set during object creation and in the Properties dialog, there are at least two other attributes that could be useful as a credential: employeeID and employeeNumber. This attribute can be viewed and set using a standard Microsoft tool, ADSI Editor. Following is an example of using the ADSI Editor tool to set the value of employeeID.

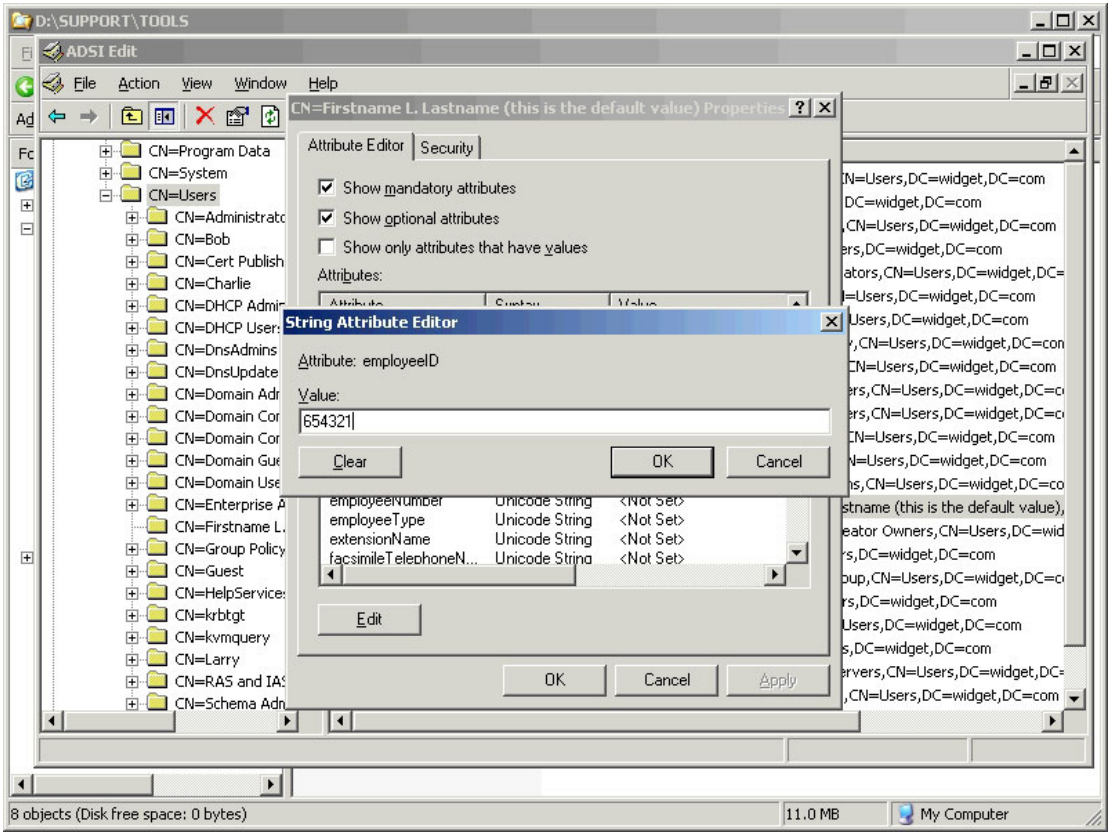

Figure B-5: ADSI Editor

UID Mask for Single Factor Credentials

The UID Mask field is used to specify which attributes are used as credentials. The default value for UID mask is shown in the following example.

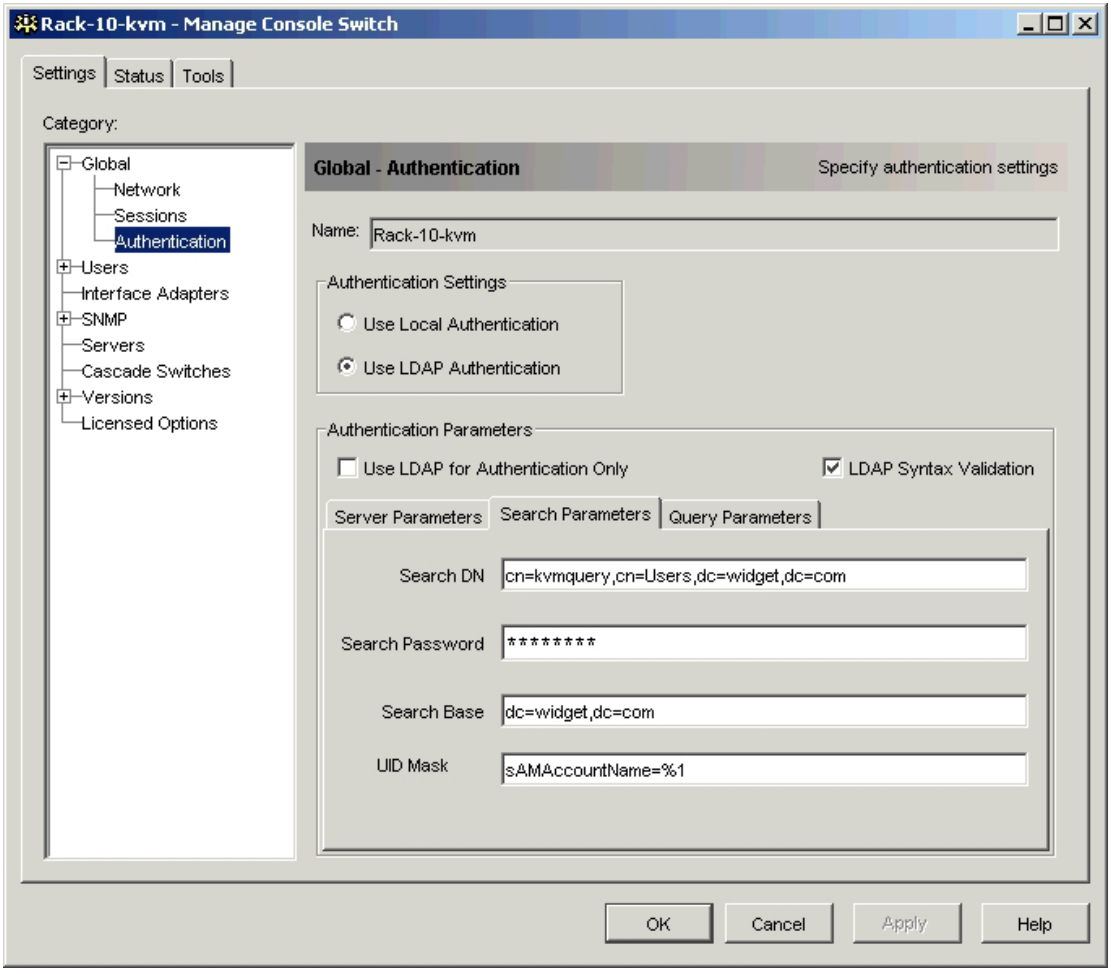

Figure B-6: Authentication Subcategory

In the preceding example, the UID mask value indicates that a single attribute, sAMAccountName, is being used in the credentials. The mask is set to %1, which refers to the first token entered by the user into the user name field of the login dialog of the client application. The contents of the user name field is parsed into tokens using the following characters as token delimiters: @, !, and &.

In the following example, the user name field contents would be parsed into two tokens: the first token is the string *anystringvalue* and the second token is *widget.com*.

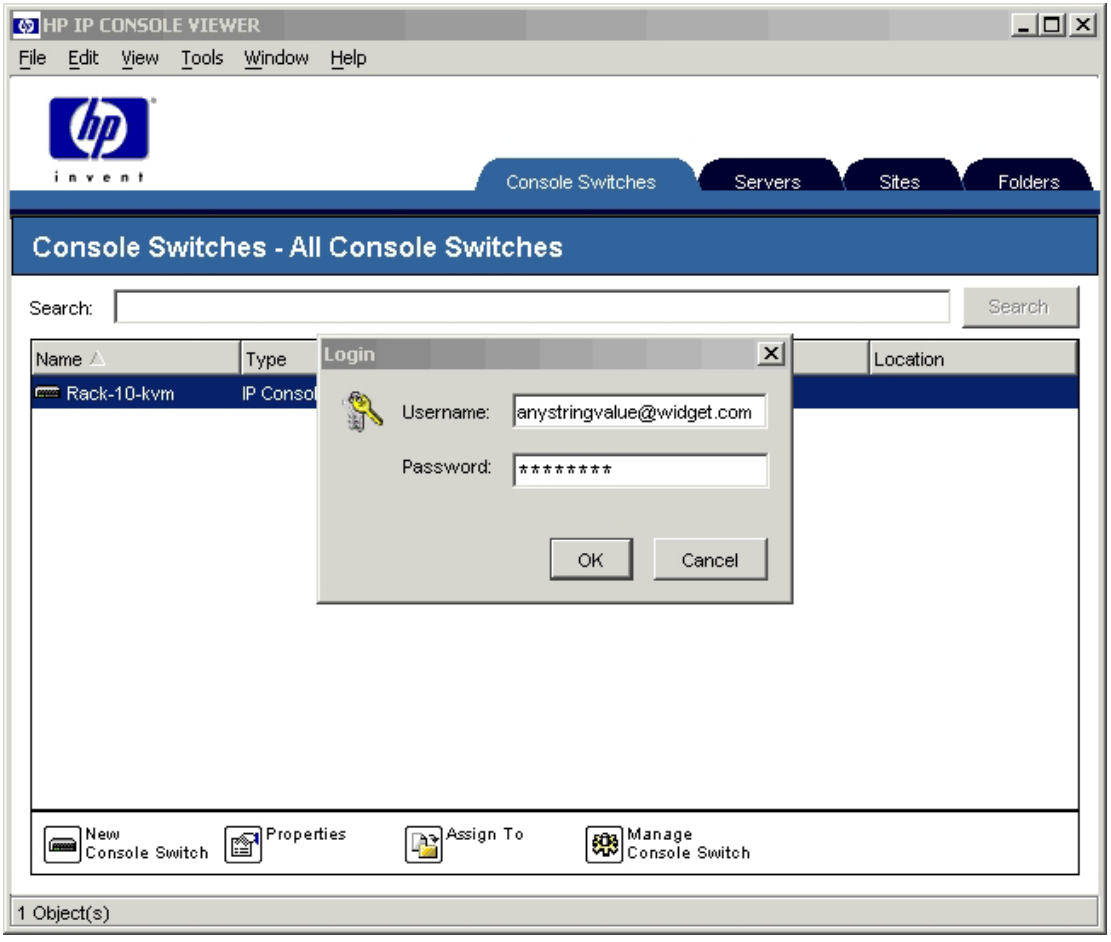

Figure B-7: Login dialog box

These two tokens are referenced in the UID mask by using the replacement parameters %1 and %2, respectively. Consider the use of User Principal Name (UPN) as an example of using two replacement parameters.

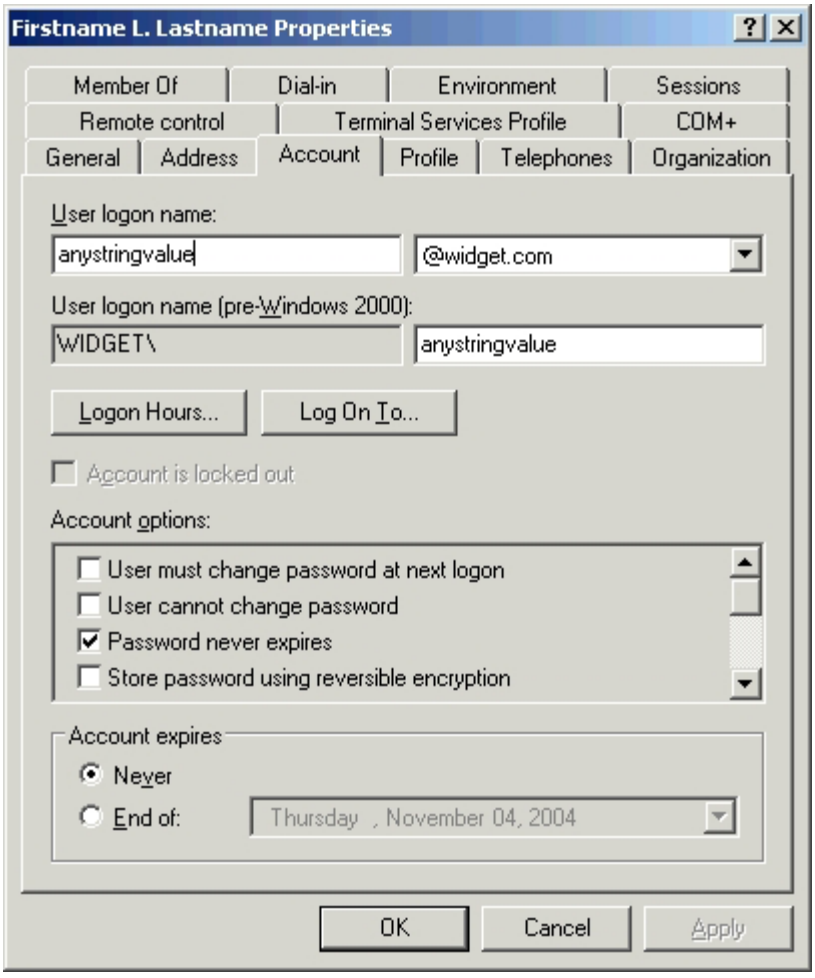

Figure B-8: Firstname L. Lastname Properties

When using UPN, the user must enter the entire UPN in the login dialog of the client application, in the User logon name field.

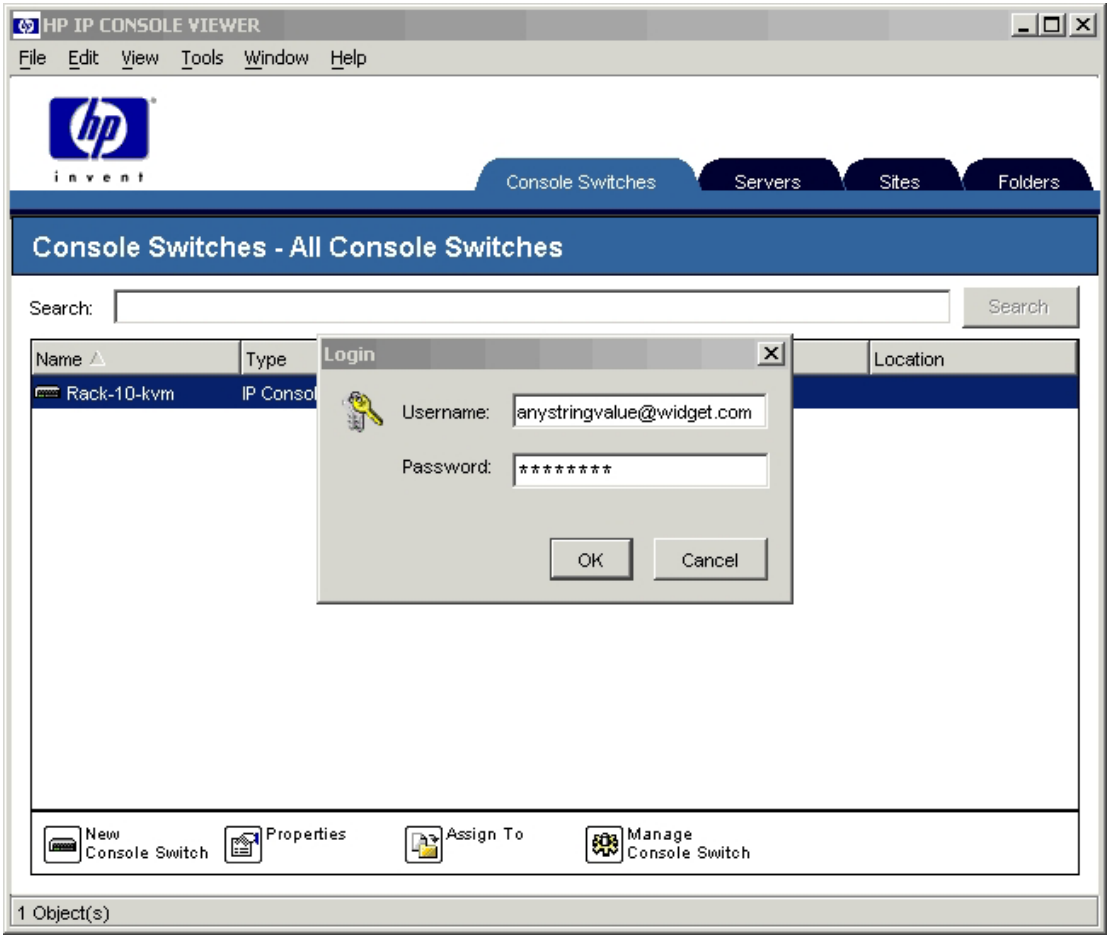

Figure B-9: Login dialog box

In this example, the console switch firmware parses the Username field into two pieces: the replacement parameter %1 gets the value “anystringvalue” and the replacement parameter %2 gets the value “widget.com.” Note that the period (.) character is not a token delimiter, and therefore widget.com is a single token.

The corresponding UID mask is shown in the following example.

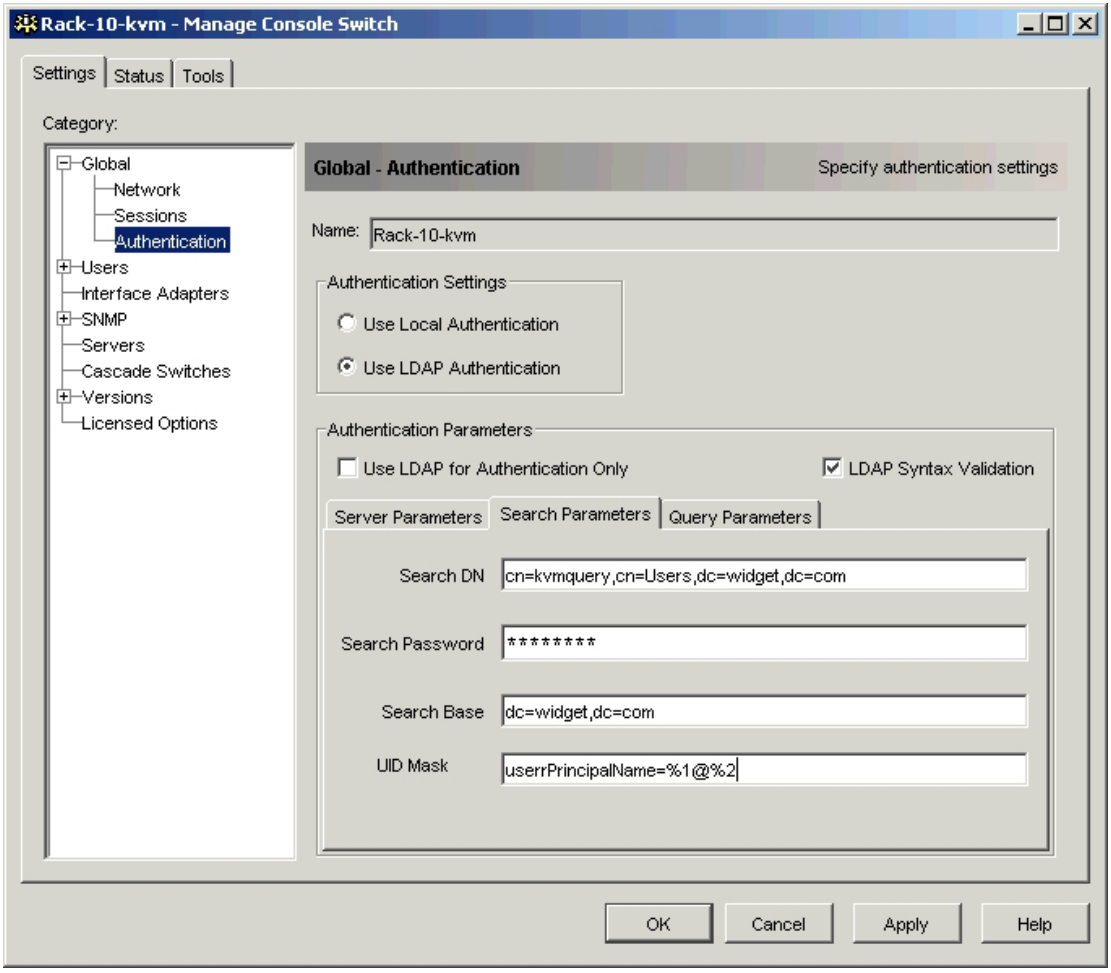

Figure B-10: Authentication Subcategory

Another valid way to UPN is to change the first part to have the form: <first name>.<last name> . The UID mask does not need to change because the period between the first name and the last name is not a token delimiter. So, the UID mask remains as in the preceding figure, while the credentials entered in the login dialog of the client application become the following.

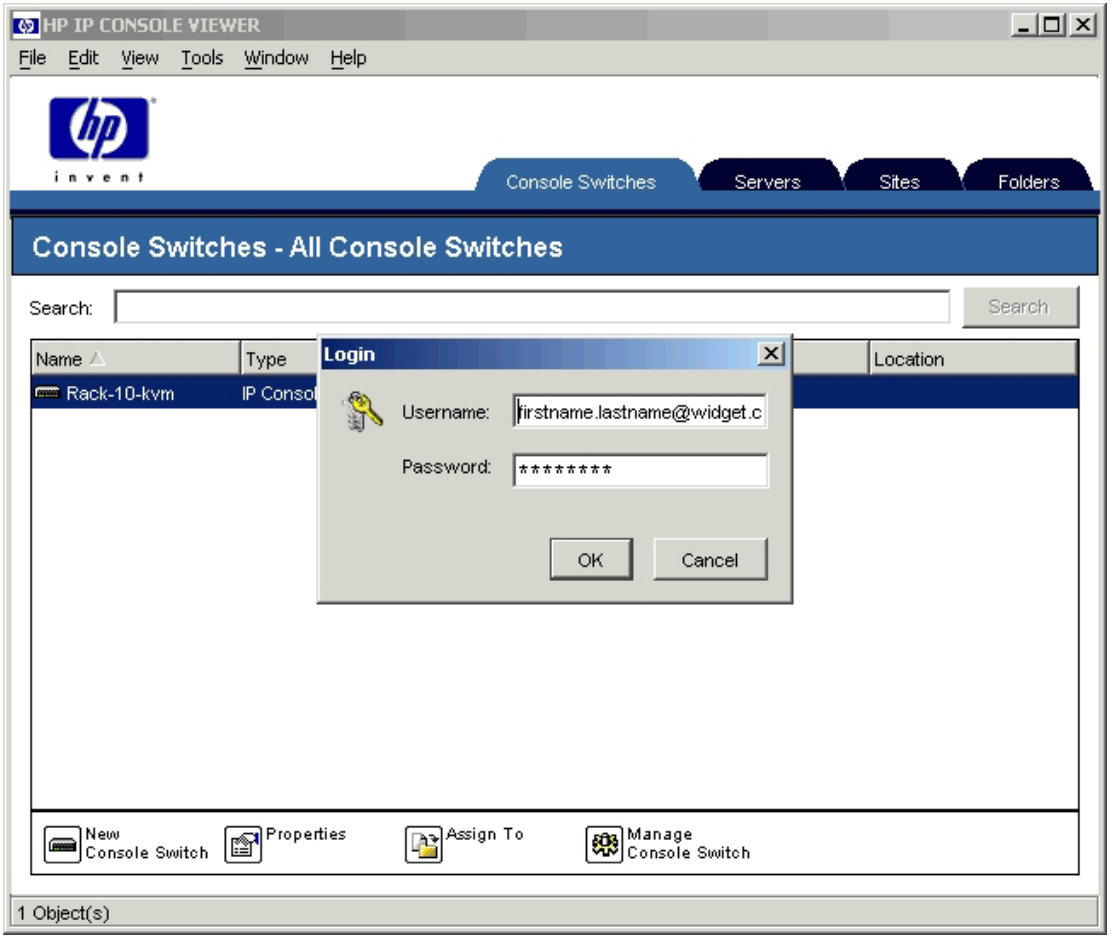

Figure B-11: Login dialog box

Of course, for this example, the user logon name would have to be changed in the AD object representing the user.

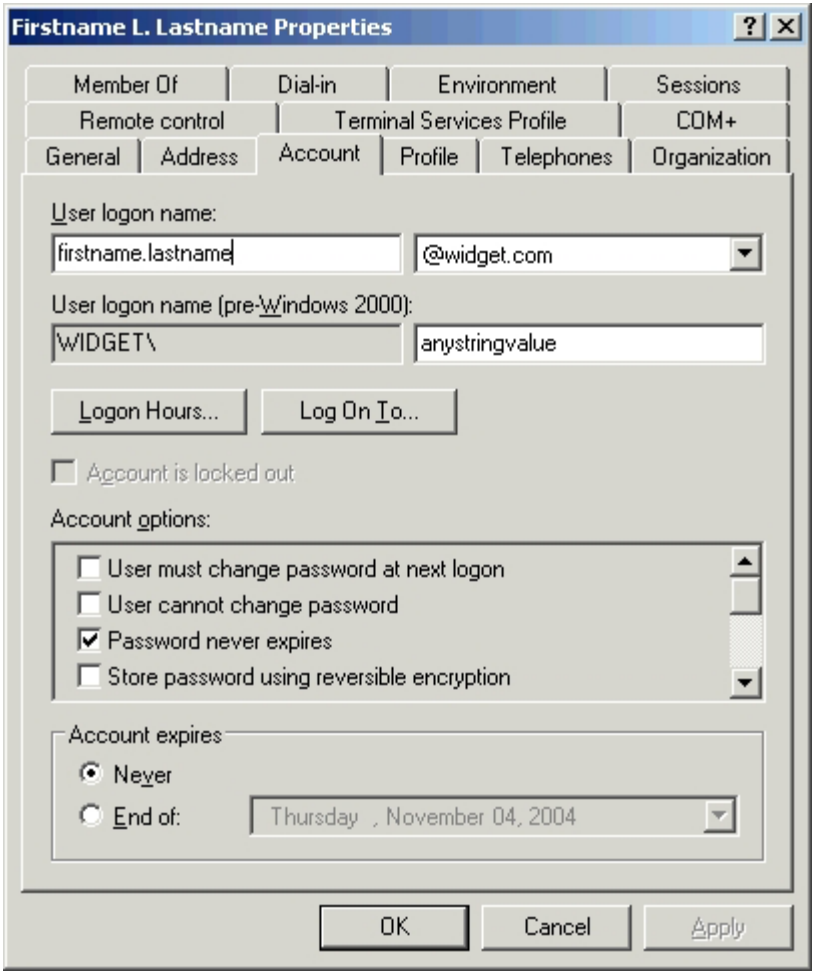

Figure B-12: Firstname L. Lastname Properties

To use the e-mail address as part of the credentials, the UID mask would be changed to the following.

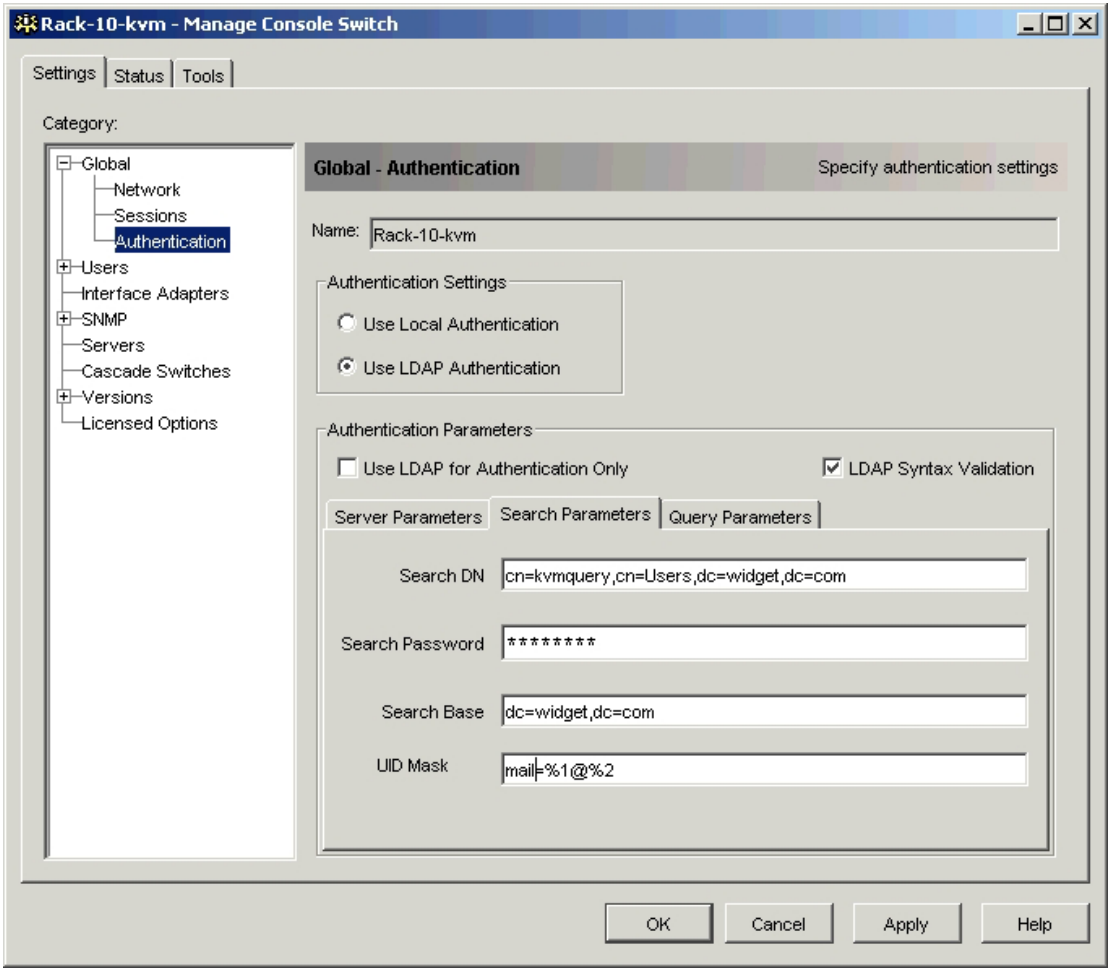

Figure B-13: Authentication Subcategory

UID Mask for Multiple Factor Credentials

For added security, an administrator might want to implement a policy that says authentication is based on UPN, password, and employeeID. In other words, the user logging in must know the UPN, password, and employeeID. The UID mask must be changed to indicate there are two attributes used as the "user name." The two attributes are separated by a # in the UID mask, as shown in the following.

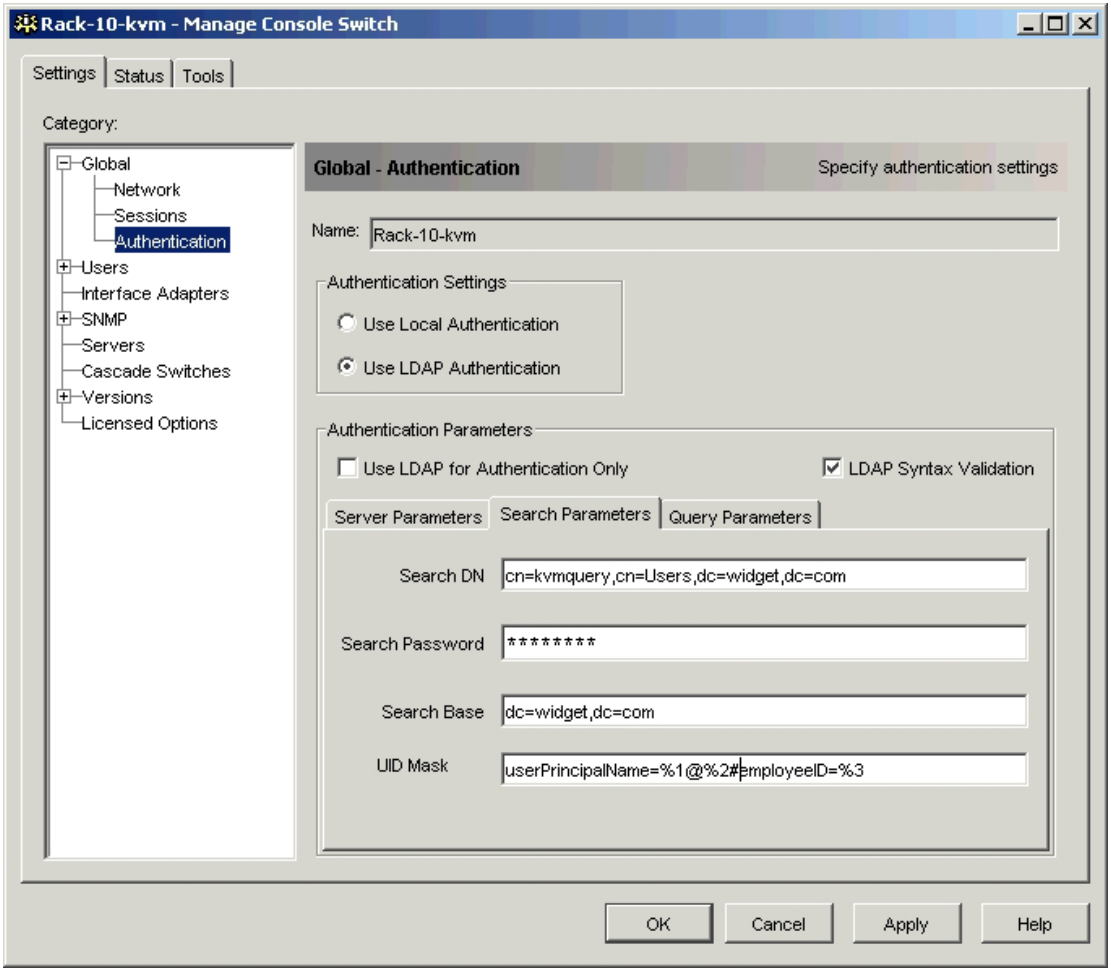

Figure B-14: Authentication Subcategory

The string entered by the user in the login dialog can be any of the following three token delimiters from which to choose.

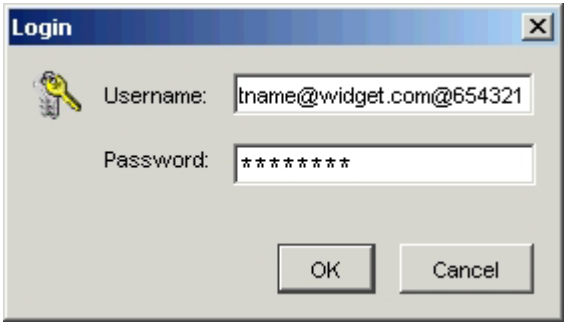

Figure B-15: Login dialog box

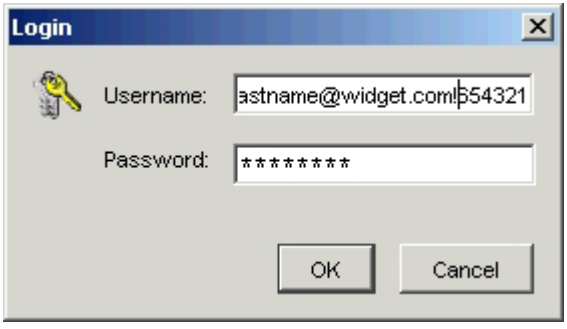

Figure B-16: Login dialog box

Figure B-17: Login dialog box

Active Directory Terminology

Active Directory (AD)
Active Directory is the latest generation of network directory services offered by Microsoft. It is supported by Windows 2000 and Windows Server 2003. As a network directory system, AD provides a highly scalable distributed repository for information about objects that reside in the network environment, such as users, computers, printers, applications, and console switches.

Active Directory Users & Computers MMC Snap-in (ADUC):
Microsoft Management Console (MMC) tool used to manage user and computer accounts in Active Directory. The tool also allows an administrator to create organizational units and other types of containers. This tool is installed automatically when AD is installed.

attribute
Each AD attribute constitutes a single property of an object stored in the AD database. An object is described by the values of its attributes. For example, one of the AD object classes is person. One of the attributes for an object of class person is named “info.” The value of the info attribute is set by entering the desired value into the Properties field, accessible by the ADUC snap-in for the MMC. Another attribute associated with person is SAM Account Name (sAMAccountName). The value of the sAMAccountName attribute is set by entering the desired value into the Logon Name field, also accessible by the ADUC. The AD schema defines the attributes associated with each object class. Each attribute has a type and one or more values. The attribute type defines the syntax of its values. The schema specifies the type of each attribute and whether it is multi-valued. See also object and LDAP Display Name.

Child Domain
A domain that is not a Domain Tree Root. See also Descendant Domains.

container

In the context of AD, the word “container” is used in two general ways. First, it is an object class defined in the schema and used in several objects created automatically when AD is installed. For example, one of these default containers is called “users,” a repository for user accounts and group objects containing user accounts. Group objects containing user accounts can be nested in various ways, so this container might hold hierarchies of groups as well as ungrouped user accounts. AD allows other types of objects to be created in the users container as well. Similarly, there is a default container called “computers” that is a repository for computer objects, groups thereof, and hierarchies of (nested) groups. Each AD install also automatically creates default container objects for information related to the database schema and the topology of the distributed AD name space used to name individual AD domains. There is no easy way to create new objects of class container. It can be accomplished but it would be unusual for an AD administrator to do so because such an object cannot have group policies applied to it. In contrast, the second kind of container, an object class known as OU, is thought of as a security boundary because it can be explicitly controlled by group policies. This property makes objects of class OU the most significant structural components that AD administrators create and use.

Continuation Reference

The LDAP searchResult that might be returned by an AD server when it holds the baseObject of a searchRequest but is unable to search all of the entries in the scope under the baseObject (that is, when some of the entries in the scope might be held in other domains). Continuation References are non-specific in the sense that the Continuation References returned in a searchResult always list all of the immediate child domains below the domain that is generating the searchResult—therefore, some of the domains listed in a response containing Continuation References might not hold any of the target objects. This is in contrast to Referrals, which are completely specific. A Referral always contains the desired baseObject of the search.

Descendant Domains

Refers collectively to all the domains below a specific root domain, without regard to whether they are immediate child domains of the root or are located lower in the contiguous name space. When it is important to emphasize that a domain is an immediate subordinate of the root, use the term “child domain.” See also Child Domain.

Directory Information Tree (DIT)

The DIT comprises the entire set of AD objects deployed by an enterprise. This set forms a tree structure in the sense that each forest tree deployed by the enterprise forms a hierarchy of AD servers whose Distinguished Names are embedded in the DNS name space, itself a tree structure. Inside each AD server, the objects form a micro-structure of hierarchically related containers and leaf objects.

Distinguished Name (DN)

Each object in the AD has a unique Distinguished Name. The DN identifies the domain that holds the object as well as the complete path through the container hierarchy (in that domain) by which the object is reached.

A typical DN might be: cn=JohnSmith, cn=users, dc=widget, dc=com.

This DN identifies the "John Smith" user object in the widget.com domain. In this example, cn is an abbreviation for common name which is an attribute. Dc is an abbreviation for domain component, which is another attribute used in AD.

domain

A single security boundary of a Windows NT-based computer network.Within a domain, objects and hierarchies of objects are created, according to the rules in the schema. A deployment of AD is made up of one or more domains. On a stand-alone workstation, the domain is the computer itself. A domain can span more than one physical location by placing peer master domain controllers at more than one site. Every domain has its own security policies and security relationships with other domains. When multiple domains are arranged to form a hierarchy beneath a root domain, the domains form a contiguous name space and are collectively referred to as a domain tree. Within a domain tree, all domains are connected by mutual trust relationships and share a common schema, configuration, and global catalog. Multiple domain trees can be connected together, in terms of trust relationships, to create a forest. Each AD host computer holds a single domain. It is not possible for a single computer to host more than one domain. It should be noted that there is a derivative product of AD, known as Active Directory Application Mode (ADAM), which does support more than one domain in a single host platform.

Domain Controller (Windows 2000 and Windows 2003 Server)

A Windows 2000-based server with Active Directory installed and enabled. The act of installing and enabling Active Directory necessarily causes a platform to become a Domain Controller. Each Domain Controller holds a single domain. A single Domain Controller cannot host more than one domain. See also Peer Master Domain Controller.

Domain Controller (pre-Windows 2000)
A Windows NT 4.0-based server configured as a Primary Domain Controller (PDC) or as a Backup Domain Controller (BDC).

Domain Name System (DNS)
The DNS is a hierarchical distributed database used for name/address translation. DNS is the name space used on the Internet to translate computer and service names into TCP/IP addresses. AD uses DNS as its location service, and so clients find domain controllers using DNS queries. AD can be used to hold the data (for example, zone and forwarding records) that constitutes the DNS database used by the DNS service running on the domain controller. When DNS records in a Domain Controller are held in its AD database, DNS zone transfers are handled as AD replication operations and DNS and AD are said to be "tightly integrated."

Domain Mode
See Mixed Domain Mode, Native Domain Mode, and Functional Levels.

Domain Tree Root
The first domain created in a Domain Tree. It might not be the Forest Root.

Domain Tree
See Domain.

forest
A group of one or more AD domain trees that mutually trust each other. All domain trees in a forest share a common schema, configuration, and global catalog. Each tree has a root domain and zero or more descendent domains, forming a contiguous name space. When a forest contains multiple trees, the trees collectively do not form a single contiguous name space. All trees in a given forest trust each other through transitive bidirectional trust relationships. Unlike a domain tree, a forest does not need a distinct name. However, the root of the first tree created in the forest is always referred to as the root of the forest. A forest exists as a set of cross-referenced objects and trust relationships known to all member trees. See also Domain and Forest Root.

Forest Root
The first domain created in an AD deployment. After the first domain is created, additional domains can be created as child domains of that root and/or as new roots of additional trees in the same forest within an enterprise AD deployment. See also forest, Domain Tree Root, and domain.

functional levels (Windows Server 2003)

Windows Server 2003 expands on the domain mode concept introduced in Windows 2000 (see Mixed Domain Mode and Native Domain Mode). Functional levels apply to both forests and domains. Like the domain mode, functional levels limit what type of operating systems can run on domain controllers in a domain or forest. Each functional level also has an associated list of features that become available when the domain or forest reaches that particular functional level. Functional levels become relevant in a domain and forest when the first domain controller running Windows Server 2003 is added to a domain. By default the domain functional level is set to "Windows 2000 Mixed", and the forest functional level is set to "Windows 2000." Functional levels can be set via the ADUC snap-in. Like domain mode, once a functional level has been elevated to a higher status, it cannot be changed back. The table below lists the operating systems that are supported by the various domain and forest functional levels.

global catalog (GC)

The global catalog contains a partial replica of every object in every domain in the forest. The GC enables users and applications to find objects in an AD forest given one or more attributes of the target object. It also contains the schema and configuration of Directory partitions. This means the GC holds a replica of every object in the AD, but with only a small number of their attributes. The attributes in the GC are those most frequently used in search operations (such as a user's first and last names, logon names, and so on). The GC enables users to find objects of interest quickly without knowing what domain holds them and without requiring a contiguous extended name space in the enterprise.The GC is built automatically by the AD replication system. Attributes can be easily added to the GC content by AD administrators.

Interim Functional Level

Interim Functional Level refers to a Windows Server 2003 configuration of AD that allows it to coexist in a domain that includes one or more Windows NT 4.0 Backup Domain Controllers. See also Functional Levels.

Lightweight Directory Access Protocol (LDAP)

LDAP is a protocol used to access a directory service such as AD that has been enabled to understand the protocol. LDAP is a simplified version of the Directory Access Protocol (DAP) developed as part of the X.500 international standard for directory services. While LDAP is certainly a computer communication protocol, the term "LDAP" is frequently used to denote more than just the protocol standard: it is inextricably tied to a default schema for the AD database and other essential aspects of interoperability.

LDAP Display Name

The name by which LDAP clients (for example, the client built into Avocent firmware) identify a specific attribute in an object. The LDAP Display Name is also an attribute in its own right and is a mandatory item in each AD object. The LDAP Display Name for an attribute contains no spaces or hyphens and the first letter is always lowercase while each distinct word in the name begins with a capital letter (for example, sAMAccountName, givenName, cn, sn). The lDAPDisplayName attribute value for each object is normally made by capitalizing the first letter of each word in the Common Name, then removing the hyphens and concatenating all the words together (and making the first letter lowercase). See also attribute.

LDAP-enabled Directory Service

A distributed network directory service that has native support for LDAP.

Mixed Domain Mode

For Windows 2000, Mixed Domain Mode refers to a configuration of AD that allows it to coexist in a domain that includes one or more Windows NT 4.0 Backup Domain Controllers. In mixed mode-the domain features from previous versions of Windows NT Server are still enabled, while some Windows 2000 features are disabled. AD domains are installed in mixed mode by default. Nested global groups are not supported in a mixed mode domain. In Mixed Mode, the AD Domain Controller emulates the behavior of a pre-Windows 2000 Primary Domain Controller (PDC) when interacting with the Backup Domain Controllers (BDCs) of that domain. See also Native Domain Mode and Functional Levels. Note: Within a multi-domain forest, running a particular domain controller in Mixed Domain Mode has no bearing in any way on any other domain. It does not matter if it is the root domain or a descendant domain because the mode only impacts the ability of that domain to replicate data to older Windows NT servers in the same domain. Running a domain controller in Mixed Domain Mode does not affect its ability to replicate and interact with Windows 2000-based servers in other domains.

Native Domain Mode

For Windows 2000, Native Domain Mode refers to a configuration of AD that allows domain controllers for a given domain to run under Windows 2000 only. For Windows Server 2003, domain controllers for a given domain are allowed to run under Windows 2000 or Windows Server 2003. This mode allows AD to enable features, such as nested global groups, that are not possible under Mixed Mode operation. See also Mixed Domain Mode and Functional Levels.

Name Space
A name or group of names that are defined according to some naming convention. Any bounded area in which a given name can be resolved. AD is primarily thought of as a name space, as is any directory service.

name resolution
Name resolution is the process of translating a name into some object or information that the name represents. AD forms a name space in which the name of an object in the directory can be resolved into the object itself.

object
An AD object is a distinct, named set of attributes that represents something concrete, such as a user, a printer, a network console switch, or an application. The attributes hold data describing the thing that is identified by the directory object. Attributes of a user might include the user's given name, surname, and e-mail address.

object class
Each object class is a structure defined in the AD schema and subsequently used to describe the attributes and other schema requirements associated with a particular type of object (for example, Object Class = User).

organizational unit (OU)
Each organizational unit created in AD is a container that is an AD administrative boundary, controlled by group policy. OUs can contain users, groups, resources, and other OUs. An OU can be thought of as providing the administrative functionality found in Windows NT 4.0 domains. In other words, the administrative control provided by Windows NT 4.0 domains has been incorporated into AD organizational units.

Peer Master Domain Controller
A Domain Controller is called a Peer Master Domain Controller if it is a controller for a domain that has more than one domain controller. It is called a "peer master" for the domain because it can be modified (unlike Backup Domain Controllers under the older Windows NT 4.0 network architecture). Each peer master for a domain replicates data modifications it receives to communicate the changes to all the other peer masters in the same domain. Under the older Windows NT 4.0 network architecture, only the Primary Domain Controller can be written to and the Backup Domain Controllers are read-only. Under Active Directory, every Domain Controller for a given domain can be written to and is responsible for replicating changes to the other Peer Master Domain Controllers for the same domain.

Referral

The LDAP searchResult returned by an LDAP server when it does not hold the base Object of a search Request. In section 4.1.11 of RFC 2251, it is referred to as an "error," and section 4.5.3 says a Referral is returned when the server has not located the baseObject and therefore has not searched any entries. A Referral is specific in the sense that it always points to a server that holds the desired baseObject (this is in contrast to Continuation References, which are non-specific in the sense that the Continuation References returned in a searchResult always list all of the immediate child domains below the domain that is generating the searchResult; therefore, some of the domains listed in a response containing Continuation References may not hold any of the target objects).

Relative Distinguished Name (RDN)

This is a term used extensively in the X.500 standards to denote the name used to uniquely reference an object relative to its parent container and the domain that holds the object In Microsoft AD, the term "RDN" is rarely used explicitly, but the concept is frequently used. It is instantiated by the rDNAttID attribute. For the object classes person, computer, and group, the value of rDNAttID is set to cn. Similarly, for the object class organizationalUnit, the value of rDNAttID is set to OU. For example, if a person distinguishedName of an object is: cn=John Smith,cn=users,dc=widget,dc=com, then that RDN of the is: cn=John Smith.

Note that in this example, the RDN appears to be the concatenation of two attribute values: the user's givenName and his surname (sn). However, in the default Microsoft AD schema, an object of class person uses the displayName attribute value as the value of the RDN of the object. In the example of John Smith, when the administrator created the user account, the Logon Name was set to JohnSmith. The Logon Name gets stored in the attribute named sAMAccountName. Note that "Logon Name" is what the field is called in the ADUC interface. Similarly, the fields in the ADUC interface labeled "First Name" and "Last Name" are stored in the attributes named givenName and sn, respectively, as well as in displayName. In Microsoft AD, for objects of class person, Common-Name (cn) and Display-Name (displayName) get assigned the same value.

root domain

A domain that is not a child domain of any domain in the forest. A root domain can have child domains. Each root domain might be a forest root. Each forest has only one root domain. See also Domain Tree Root and Forest Root.

SAM Account Name

See Relative Distinguished Name.

schema

The rules used to control the structure of AD data within a domain. The schema defines the object classes that can be used to create objects in a domain. For each object class, the schema defines exactly what attributes an instance of that class must have, what additional attributes it may have, and what object class can be its parent within nested hierarchies. Within an AD forest, all domains have the same schema. How objects may be arranged in hierarchical relationships within a domain is left to the discretion of each vendor selling an LDAP-enabled Directory Service product. The default hierarchies allowed by each vendor are controlled by that vendor's default schema.

subdomains

Same as Descendant Domains.

Tree Depth

Refers to the number of generational levels in a specific subtree of a specific domain. For a given forest, the forest root domain is said to be at Tree Depth = 1. The immediate child domains of the forest root, if any, are said to be at Tree Depth =2, and similarly for subsequent generations below the immediate child domains of the forest root. A forest may have more than one tree (that is, more than one root domain), although only one of them is known as the forest root. Each root domain in a forest is said to be at Tree Depth = 1. The scheme for numbering tree depth is the same for all trees in a forest. It is the same as for the tree whose root is the forest root domain.

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W